6 10/100/1000T + 2 10/100/1000T/ 100/1000 SFP Combo w/ X-Ring Managed Industrial Switch

User Manual

SISGM1040-162D

TRANSITION NETWORKS®

Notice

The contents of this manual are based on the table below listing firmware version, software kernel version, and hardware version. If the switch functions are different from the description of the manual, please contact the local sale dealer for more information.

Firmware Version	V1.00
Kernel Version	V1.61
Hardware Version	---------

FCC Warning

This Equipment has been tested and found to comply with the limits for a Class-A digital device, pursuant to Part 15 of the FCC rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses, and can radiate radio frequency energy. It may cause harmful interference to radio communications if the equipment is not installed and used in accordance with the instructions. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

- Reorient or relocate the receiving antenna.
- Increase the separation between the equipment and receiver.
- Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.
- Consult the dealer or an experienced radio/TV technician for help.

CE Mark Warning

This is a Class-A product. In a domestic environment this product may cause radio interference in which case the user may be required to take adequate measures.

Content

Introduction 1

Benefits 1

Package Contents 3

Hardware Description 4

Physical Dimension 4

Front Panel 4

Top View 5

LED Indicators 5

Wiring the Power Inputs 7

Wiring the Fault Alarm Contact 8

Mounting Installation 9

DIN-Rail Mounting 9

Wall Mount Plate Mounting 11

Hardware Installation 12

Installation Steps 12

Network Application 13

X-Ring Application 14

Coupling Ring Application 15

Dual Homing Application 16

Console Management 17

Connecting to the Console Port 17

Pin Assignment 17

Login in the Console Interface 18

CLI Management 19

Commands Level 20
Commands Set List 21
System Commands Set 21
Port Commands Set 24
Trunk Commands Set 26
VLAN Commands Set 28
Spanning Tree Commands Set 29
QOS Commands Set 32
IGMP Commands Set 33
Mac / Filter Table Commands Set 33
SNMP Commands Set 34
Port Mirroring Commands Set 37
802.1x Commands Set 37
TFTP Commands Set 39
SystemLog, SMTP and Event Commands Set 40
SNTP Commands Set 42
X-ring Commands Set 43
Web-Based Management 45
About Web-based Management 45
Preparing for Web Management 45
System Login 46
Main Page 47
System Information 48
IP Configuration 49
DHCP Server—System configuration 50
DHCP Client—Client Entries 51
DHCP Server—Port and IP Bindings 52

TFTP—Update Firmware 53
TFTP—Restore Configuration 54
TFTP—Backup Configuration 55
System Event Log—Syslog Configuration 56
System Event Log—SMTP Configuration 57
System Event Log—Event Configuration 59
Fault Relay Alarm 61
SNTP Configuration 62
IP Security 65
User Authentication 67
Port Statistics 68
Port Control 69
Port Trunk 70
Aggregator setting 70
Aggregator Information 72
State Activity 73
Port Mirroring 74
Rate Limiting 75
VLAN configuration 76
VLAN configuration—Port-based VLAN 77
802.1Q VLAN 79
Rapid Spanning Tree 82
RSTP - System Configuration 82
RSTP - Port Configuration 84
SNMP Configuration 86
System Configuration 86

Trap Configuration 88
SNMPV3 Configuration 89
QoS Configuration 92
QoS Policy and Priority Type 92
Port Base Priority 94
COS Configuration 94
TOS Configuration 94
IGMP Configuration 95
X-Ring 97
LLDP Configuration 99
Security 100
802.1X/Radius Configuration 100
MAC Address Table 104
Factory Default 108
Save Configuration 109
System Reboot 110
Troubles shooting 111
Technical Specification 112
Appendix 117
10 /100BASE-TX Pin outs 117
10/100Base-TX Cable Schematic 117
10/100/1000Base-TX Pin outs 118
10/100/1000Base-TX Cable Schematic 119
Gigabit Copper/SFP (mini-GBIC) combo port 120
Cabling 124

Introduction

The 6 10/100/1000T + 2 10/100/1000T/ 100/1000 SFP Combo w/ X-Ring Managed Switch is a cost-effective solution and meets the high reliability requirements demanded by industrial applications. The 6 10/100/1000T + 2 10/100/1000T/ 100/1000 SFP Combo w/ X-Ring Managed Switch can be easily managed through the Web GUI. The fiber port can extend the connection distance to increase network elasticity and performance. It also provides the X-Ring function that can prevent network connection failure.

Benefits

- System Interface/Performance
  - RJ-45 ports support auto MDI/MDI-X function
  - SFP (Mini-GBIC) supports 100/1000 Dual Mode
  - Store-and-Forward switching architecture
  - Back-plane (Switching Fabric): 16Gbps
  - 1Mbits Packet Buffer
  - 8K MAC Address Table
- Power Supply
  - Input Power Isolation design for Telecom application, Pass Hi-Pot test~1.5KV
  - Wide-range Redundant Power Design
- VLAN
  - Port Based VLAN
  - Supports 802.1Q Tag VLAN
  - GVRP
  - Double Tag VLAN (Q in Q)*
- Port Trunk with LACP
- Supports 802.1ab LLDP
- QoS (Quality of Service)
  - Supports IEEE 802.1p Class of Service
  - Per port provides 4 priority queues
  - Port Base, Tag Base and Type of Service Priority

- Port Mirror: Monitor traffic in switched networks
  - TX Packet only
  - RX Packet only
  - Both of TX and RX Packet
- Security
  - Port Security: MAC address entries/filter
  - IP Security: IP address security management to prevent unauthorized intruder
  - Login Security: IEEE 802.1X/RADIUS
- IGMP with Query mode for Multi Media Application
- Case/Installation
  - IP-30 Protection
  - DIN Rail and Wall Mount Design
- Spanning Tree
  - Support IEEE 802.1d Spanning Tree
  - Support IEEE 802.1w Rapid Spanning Tree
- X-ring
  - X-ring, Dual Homing, and Couple Ring Topology
  - Provide redundant backup feature and the recovery time below 20ms
- Bandwidth Control
  - Ingress Packet Filter and Egress Rate Limit
  - Broadcast/Multicast Packet Filter Control
- System Event Log
  - System Log Server/Client
  - SMTP e-mail Alert
  - Relay Alarm Output System Events
- SNMP Trap
  - Device cold start
  - Power status
  - Authentication failure
  - X-ring topology changed
  - Port Link up/Link down
- TFTP Firmware Update and System Configuration Restore and Backup

Package Contents

Please refer to the package content list below to verify them against the checklist.

- 6 10/100/1000T + 2 10/100/1000T/ 100/1000 SFP Combo w/ X-Ring Managed Switch
- User manual
- RS-232/RJ-45 cable
- Pluggable Terminal Block
- 2 wall mount plates and 6 screws
- One DIN-Rail (attached on the switch)

Compare the contents of the industrial switch with the standard checklist above. If any item is damaged or missing, please contact the local dealer for service.

Hardware Description

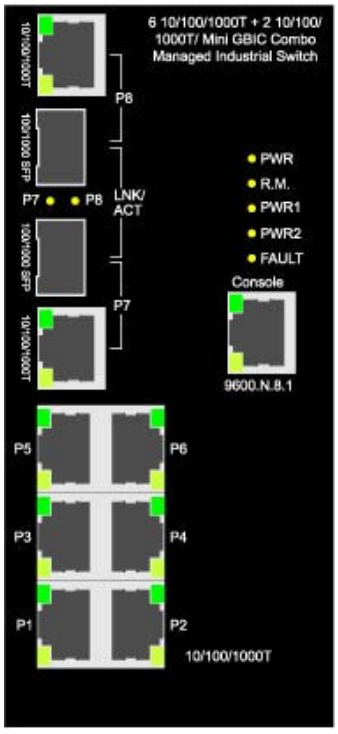
This section describes the Industrial switch's hardware spec, port, cabling information, and wiring installation.

Physical Dimension

6 10/100/1000T + 2 10/100/1000T/ 100/1000 SFP Combo w/ X-Ring Managed Switch dimension (W x D x H) is **72mm x 105mm x 152mm**

Front Panel

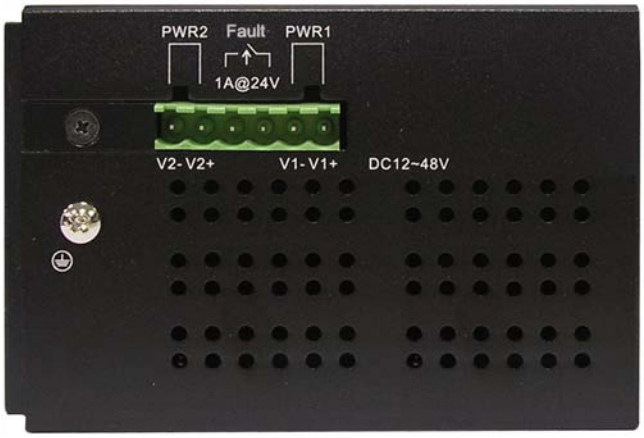
Shown below is the front panel of the 6 10/100/1000T + 2 10/100/1000T/ 100/1000 SFP Combo w/ X-Ring Managed Switch.



Front Panel of the industrial switch

Top View

The top panel of the 6 10/100/1000T + 2 10/100/1000T/ 100/1000 SFP Combo w/ X-Ring Managed Switch has one terminal block connector for two DC power inputs.



Top Panel of the industrial switch

LED Indicators

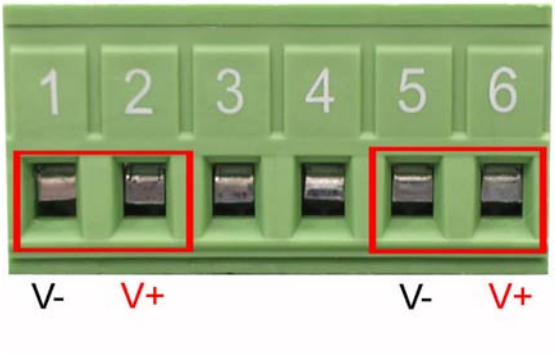
There are diagnostic LED indicators located on the front panel of the industrial switch. They provide real-time information of system and optional status. The following table provides description of the LED status and their meanings for the switch.

LED	Status	Description
PWR	Green	System power on
	Off	No power input
R.M.	Green	The industrial switch is the master of the X-Ring group
	Off	The industrial switch is not the ring master in the X-Ring group
PWR1	Green	Power input 1 is active

	Off	Power input 1 is inactive
PWR2	Green	Power input 2 is active
	Off	Power input 2 is inactive
Fault	Red	Power input 1 or 2 is inactive or port link failure (depends on Fault Relay Alarm configuration)
	Off	Power input 1 and 2 are both active, or no power inputs
LNK/ACT (for P7, P8 SFP)	Green	SFP port is linking
	Blinking	Data is transmitting or receiving
	Off	Not connected to network
P1 ~ P8 (RJ-45)	Green (upper LED)	Connected to network
	Blinking (upper LED)	Networking is active
	Off (lower LED)	No connected to network
	Green (lower LED)	The port is operating at speed of 1000M
	Off (lower LED)	The port is disconnected or working at speed of 10/100M

Wiring the Power Inputs

Please follow the steps below to insert the power wire.



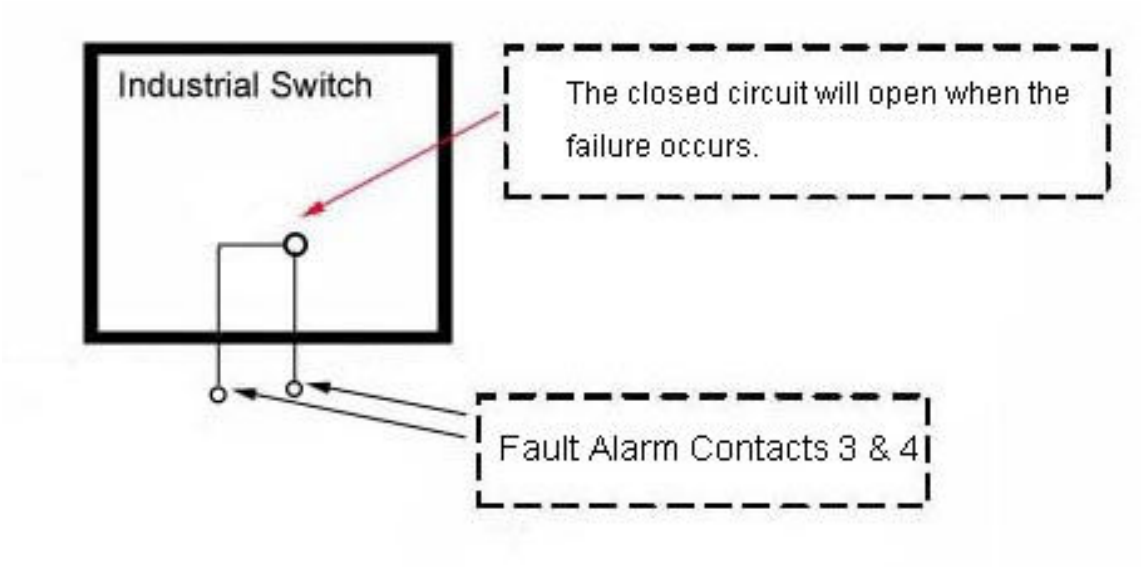
Insert the positive and negative wires into the V+ and V- contacts on the terminal block connector.

Tighten the wire-clamp screws for preventing the wires from loosing.

Wiring the Fault Alarm Contact

The fault alarm contacts are in the middle of the terminal block connector as the picture shows below. The switch will provide local indication of a power or port failure, if configured, by opening the relay contacts. The following illustration shows an application example for wiring the fault alarm contacts.

Insert the wires into the fault alarm contacts (No. 3 & 4)

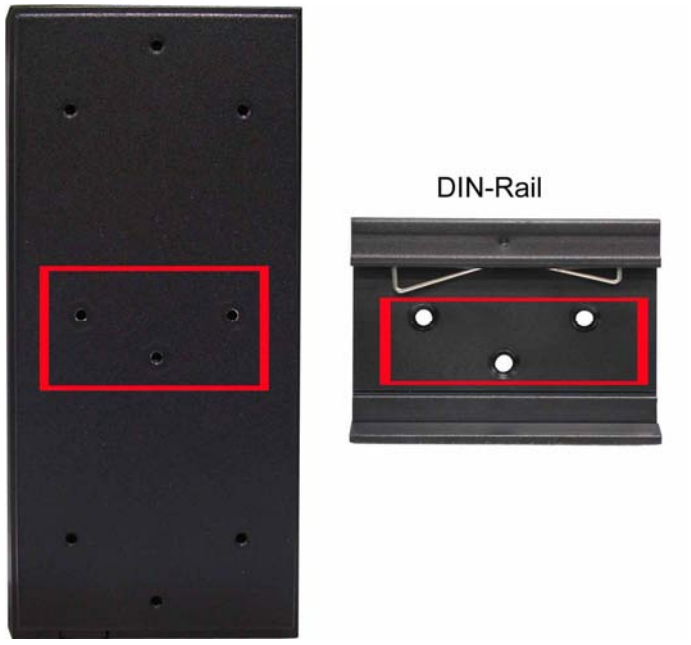


Note	*The wire gauge for the terminal block should be in the range between 12~ 24 AWG.*

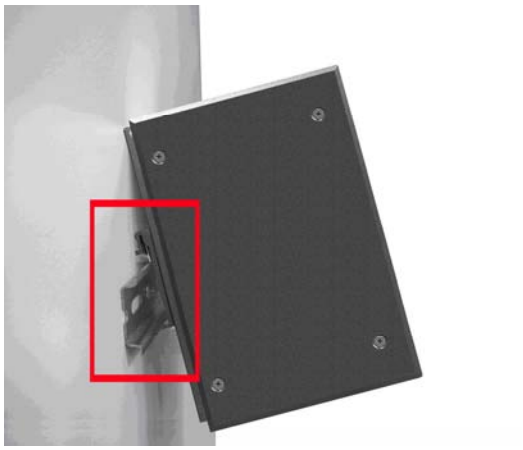
Mounting Installation

DIN-Rail Mounting

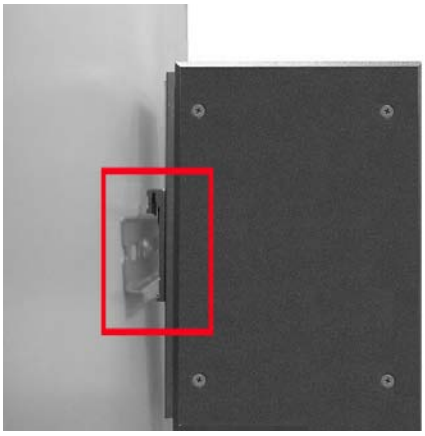
The DIN-Rail is installed on the industrial switch at the factory. If the DIN-Rail is not installed, please see the following pictures to screw the DIN-Rail onto the switch. Follow the steps below to hang the industrial switch.



1. First, insert the top of DIN-Rail into the track.



2. Then, lightly push the DIN-Rail into the track.

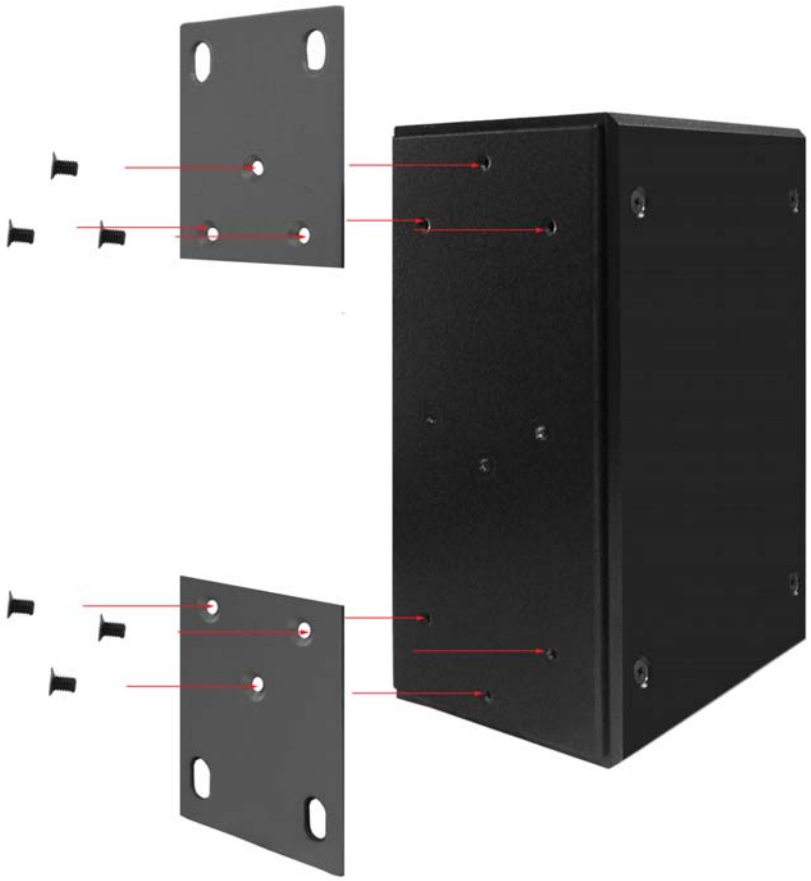


3. Check if the DIN-Rail is tightened on the track or not.
4. To remove the industrial switch from the track, reverse steps above.

Wall Mount Plate Mounting

Follow the steps below to mount the industrial switch with a wall mount plate.

1. Remove the DIN-Rail from the industrial switch; loose the screws to remove the DIN-Rail.
2. Place the wall mount plate on the rear panel of the industrial switch.
3. Use the screws to screw the wall mount plate on the industrial switch.
4. Use the hook holes at the corners of the wall mount plate to hang the industrial switch on the wall.
5. To remove the wall mount plate, reverse the steps above.



Screwing the wall mount plate on the Industrial Switch

Hardware Installation

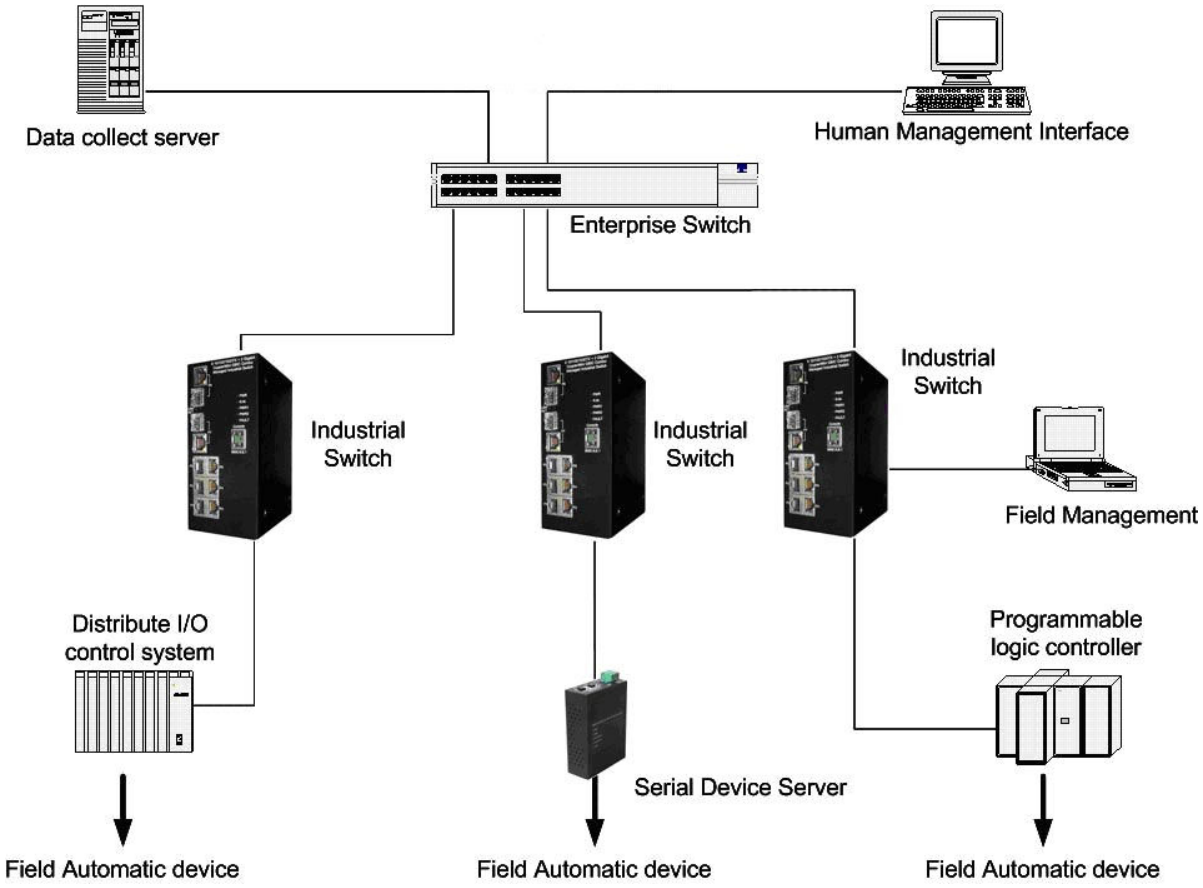
This section describes how to physically install the 6 10/100/1000T + 2 10/100/1000T/ 100/1000 SFP Combo w/ X-Ring Managed Switch.

Installation Steps

1. Unpack the Industrial switch.
2. Check if the DIN-Rail is screwed on the Industrial switch or not. If not, please refer to **DIN-Rail Mounting** section for DIN-Rail installation. If user wants to wall mount the Industrial switch, please refer to **Wall Mount Plate Mounting** section for wall mount plate installation.
3. To hang the Industrial switch on the DIN-Rail track or wall, please refer to the **Mounting Installation** section.
4. Power on the Industrial switch. Please refer to the **Wiring the Power Inputs** section for information about how to wire the power. The power LED on the Industrial switch will light up. Please refer to the **LED Indicators** section for indication of LED lights.
5. Prepare the twisted-pair, straight through Category 5e/above cable for Ethernet connection.
6. Insert one side of RJ-45 cable into the Industrial switch Ethernet port (RJ-45 port) and another side of RJ-45 cable to the network device's Ethernet port (RJ-45 port), e.g. Switch, PC or Server. The UTP port (RJ-45) LED on the industrial switch will light up when the cable is connected with the network device. Please refer to the **LED Indicators** section for LED light indication.
7. When all connections are set and LED lights indicate normal operation, the installation is complete.

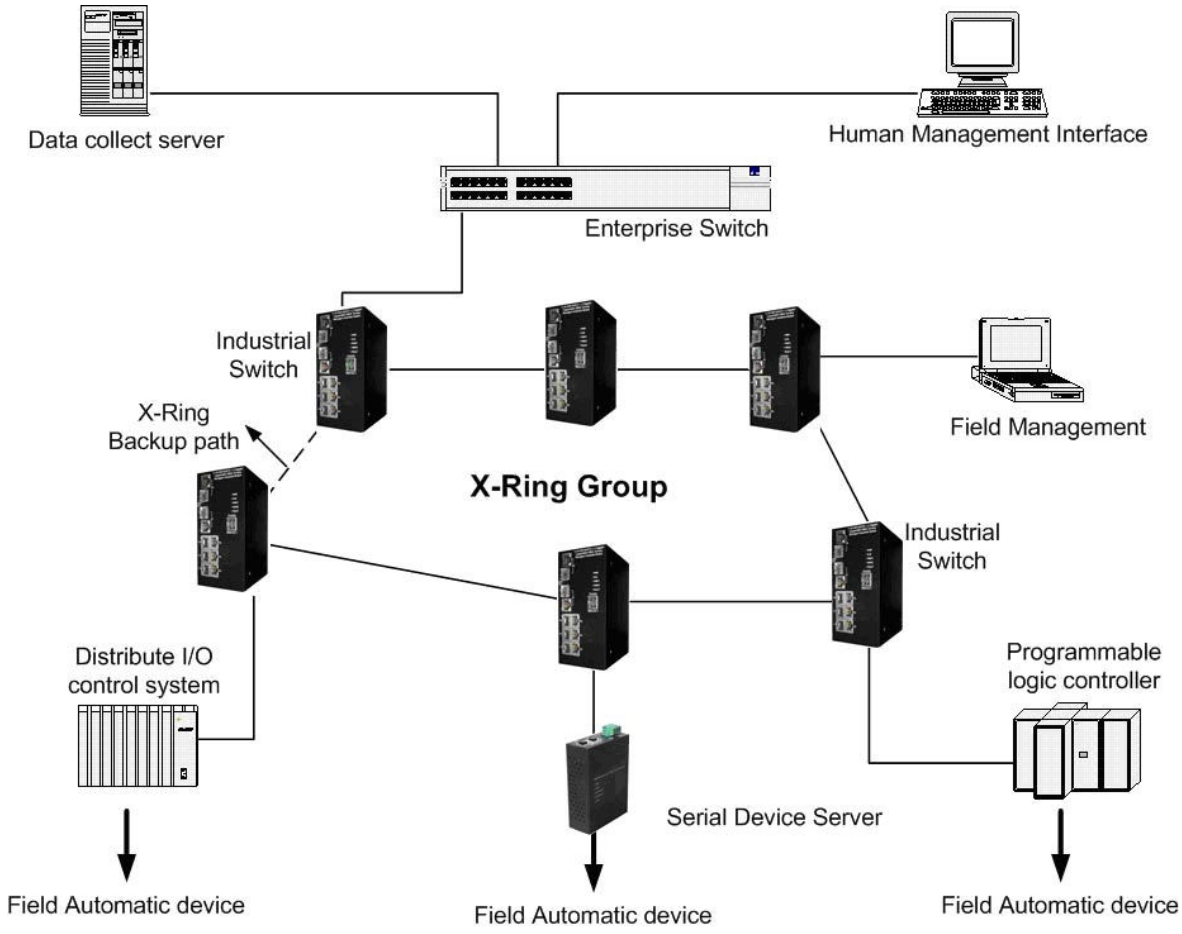
Network Application

This section provides some sample applications to guide users. A sample application of the industrial switch is shown as below:



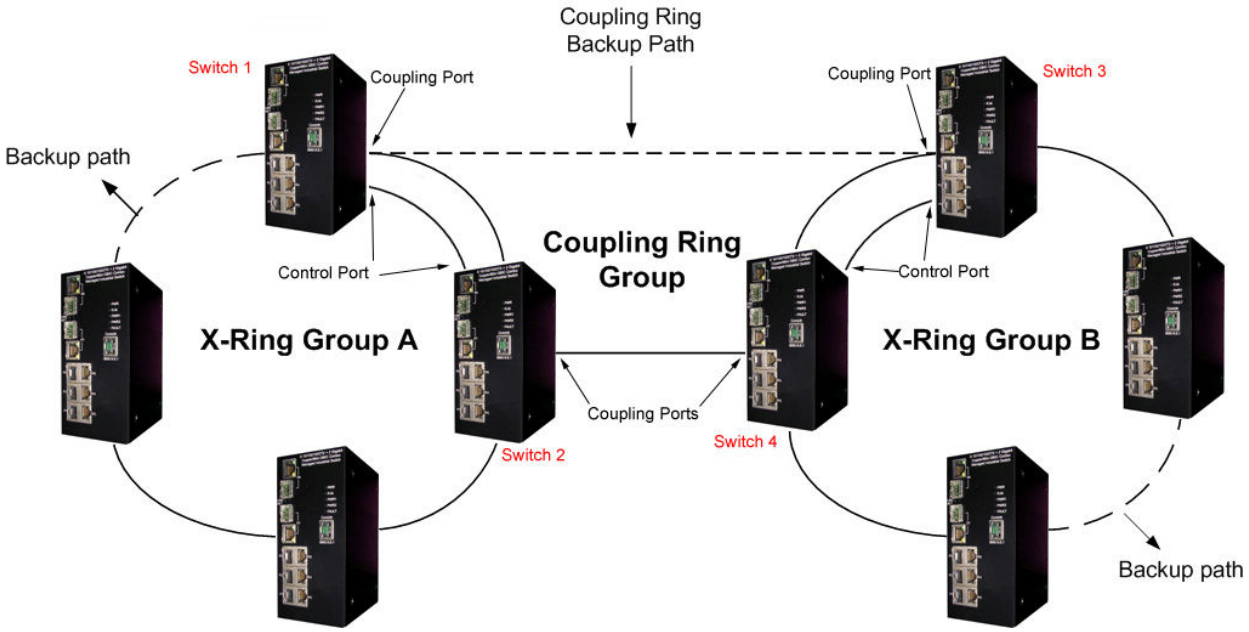
X-Ring Application

The industrial switch supports the X-Ring protocol that can help the network recover from a connection failure within 300ms or less, ensuring network reliability. The X-Ring algorithm is similar to Spanning Tree Protocol (STP)/RSTP algorithm but its recovery time is less than STP/RSTP. The following figure illustrates an X-Ring application.



Coupling Ring Application

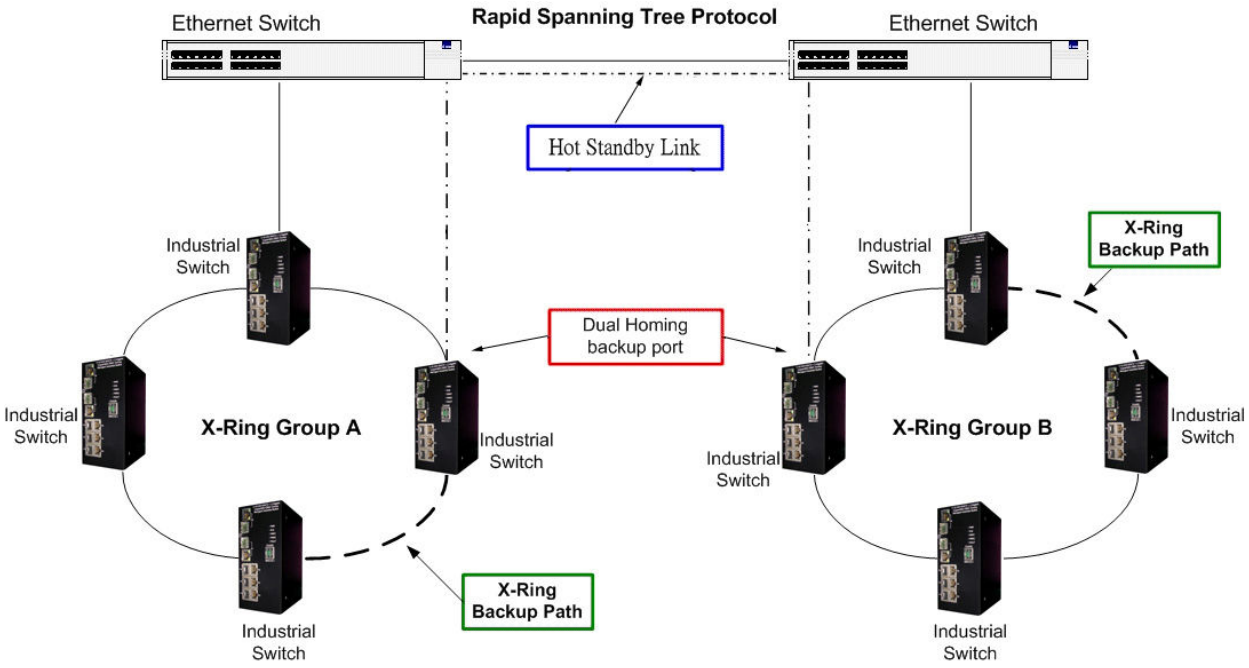
In the network, there may be more than one X-Ring group. The coupling ring function can connect each X-Ring for redundant backup. It can ensure transmissions between two ring groups do not fail. The following figure is a sample coupling ring application.



Dual Homing Application

Dual Homing is a function to prevent the connection breaking between an X-Ring group and an upper level/core switch. Assign two ports to be the Dual Homing port that is the backup port in an X-Ring group. The Dual Homing function works only when the X-Ring function is active. Each X-Ring group has only one Dual Homing port.

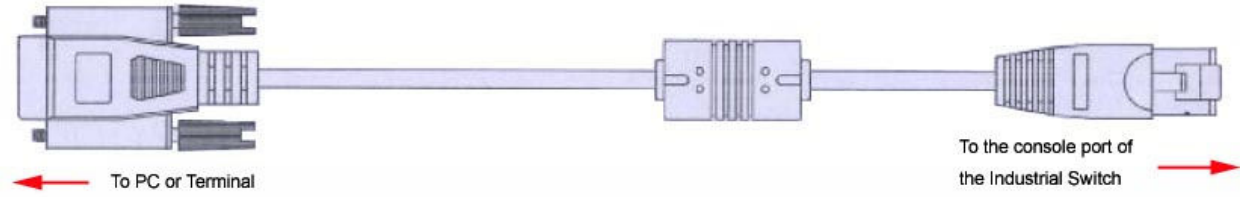
[NOTE] In a Dual Homing application architecture, the Rapid Spanning Tree protocol of the upper level switches must be enabled.

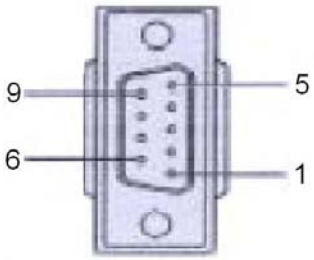


Console Management

Connecting to the Console Port

The supplied cable has an RS-232 connector on one end and an RJ-45 connector on the other. Attach the end with the RS-232 connector to a PC or terminal and the other end with the RJ-45 connector to the console port of the switch. The connected terminal or PC must support the terminal emulation program.





DB 9-pin Female

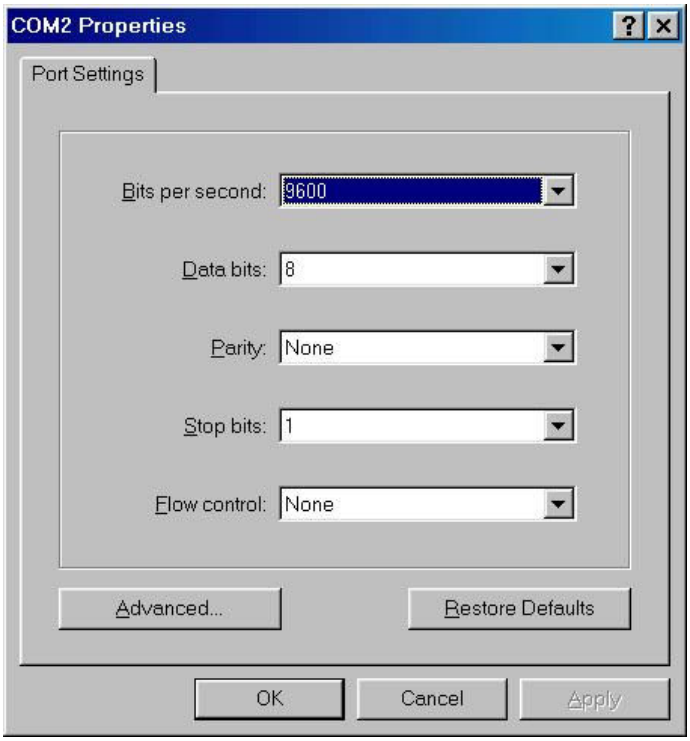
Pin Assignment

DB9 Connector	RJ-45 Connector	
NC	1	Orange/White
2	2	Orange
3	3	Green/White
NC	4	Blue
5	5	Blue/White
NC	6	Green
NC	7	Brown/White
NC	8	Brown

Login in the Console Interface

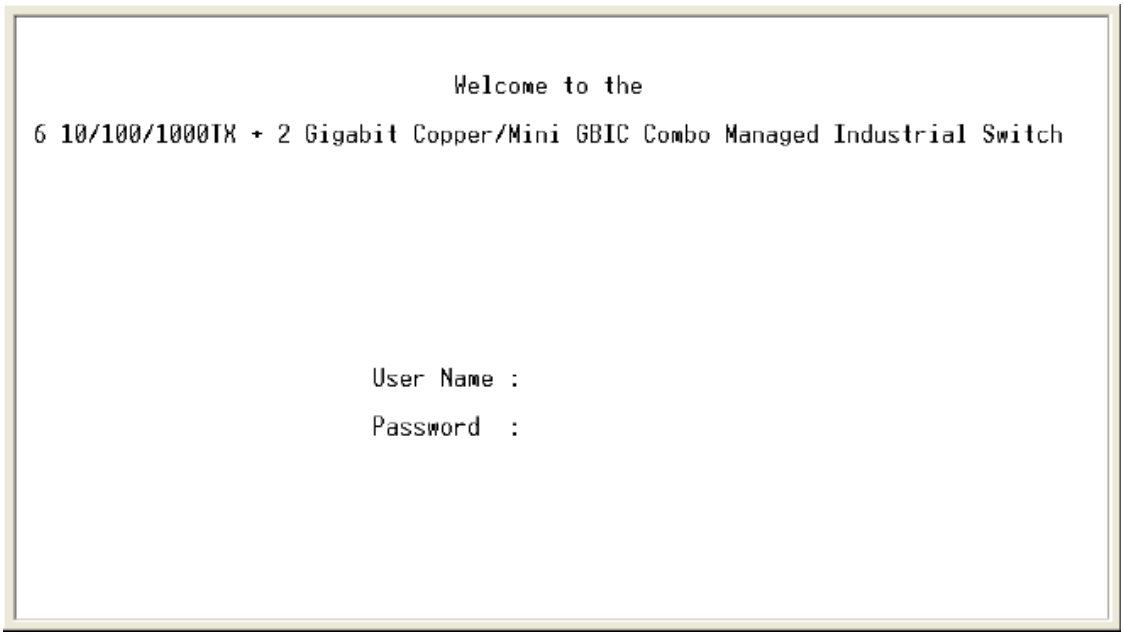
When the connection between Switch and PC is ready, turn on the PC and run a terminal emulation program or **Hyper Terminal** and configure its **communication parameters** to match the following default characteristics of the console port:

Baud Rate: 9600 bps
Data Bits: 8
Parity: none
Stop Bit: 1
Flow control: None



The settings of communication parameters

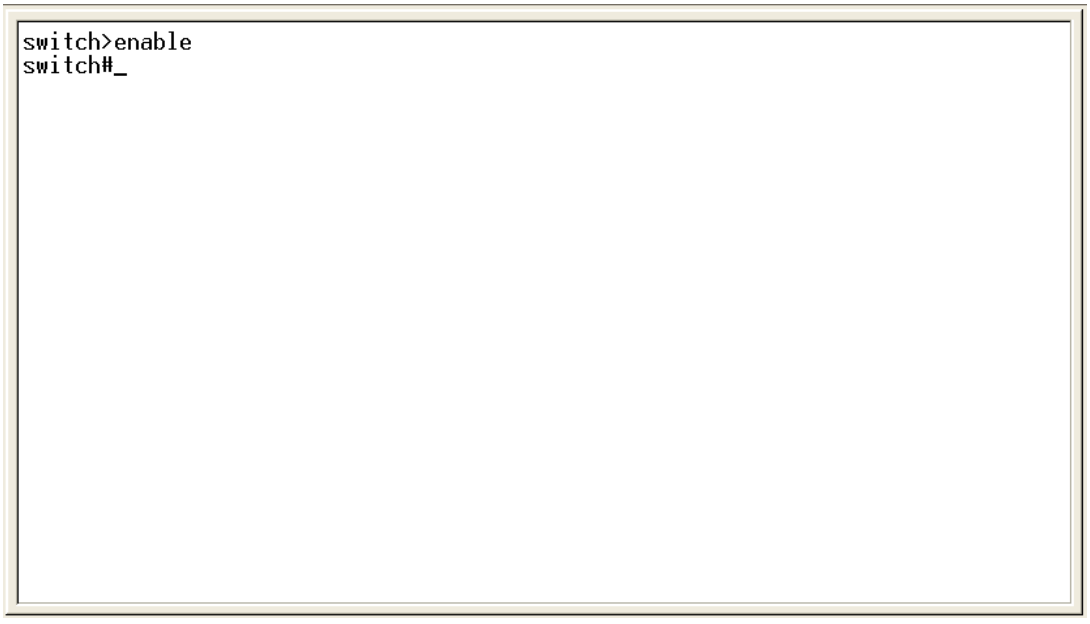
After finishing the parameter settings, click "**OK**". When the blank screen shows up, press **Enter** key to bring out the login prompt. Key in the "**root**"(default value) for the both User name and Password (use **Enter** key to switch), then press **Enter** key and the Main Menu of console management appears. Please see the figure as below.



Console login interface

CLI Management

The system supports a command line interface management–CLI. After you have logged in the system by typing in user name and password, you will see a command prompt. To enter CLI management interface, enter "**enable**" command.



CLI command interface

The following table lists the CLI commands and description.

Commands Level

Modes	Access Method	Prompt	Exit Method	About This Mode1
User EXEC	Begin a session with your switch.	switch>	Enter logout or quit.	The user commands available at the user level are a subset of those available at the privileged level. Use this mode to • Perform basic tests. • Displays system information.
Privileged EXEC	Enter the enable command while in user EXEC mode.	switch#	Enter disable to exit.	The privileged command is advance mode Privileged this mode to • Displays advance function status • Save configures
Global Configuration	Enter the configure command while in privileged EXEC mode.	switch (config)#	To exit to privileged EXEC mode, enter exit or end	Use this mode to configure parameters that apply to your switch as a whole.
VLAN database	Enter the vlan database command while in privileged	switch (vlan)#	To exit to user EXEC mode, enter exit.	Use this mode to configure VLAN-specific parameters.

	EXEC mode.			
Interface configuration	Enter the interface command (with a specific interface) while in global configuration mode	switch (config-if)#	To exit to global configuration mode, enter exit. To exist to privileged EXEC mode, or end.	Use this mode to configure parameters for the switch and Ethernet ports.

User EXEC	**E**
Privileged EXEC	**P**
Global configuration	**G**
VLAN database	**V**
Interface configuration	**I**

Commands Set List

System Commands Set

Netstar Commands	Level	Description	Example
show config	**E**	Show switch configuration	switch>**show config**
show terminal	**P**	Show console information	switch#**show terminal**
write memory	**P**	Save user configuration into permanent memory (flash rom)	switch#**write memory**
system name [System Name]	**G**	Configure system name	switch(config)#**system name xxx**
system location	**G**	Set switch system	switch(config)#**system location**

[System Location]		location string	**xxx**
system description [System Description]	**G**	Set switch system description string	switch(config)#**system description xxx**
system contact [System Contact]	**G**	Set switch system contact window string	switch(config)#**system contact xxx**
show system-info	**E**	Show system information	switch>**show system-info**
ip address [Ip-address] [Subnet-mask] [Gateway]	**G**	Configure the IP address of switch	switch(config)#**ip address 192.168.16.1 255.255.255.0 192.168.16.254**
ip dhcp	**G**	Enable DHCP client function of switch	switch(config)#**ip dhcp**
show ip	**P**	Show IP information of switch	switch#**show ip**
no ip dhcp	**G**	Disable DHCP client function of switch	switch(config)#**no ip dhcp**
reload	**G**	Halt and perform a cold restart	switch(config)#**reload**
default	**G**	Restore to default	switch(config)#**default**
admin username [Username]	**G**	Changes a login username. (maximum 10 words)	switch(config)#**admin username xxxxxx**
admin password [Password]	**G**	Specifies a password (maximum 10 words)	switch(config)#**admin password xxxxxx**
show admin	**P**	Show administrator information	switch#**show admin**
dhcpserver enable	**G**	Enable DHCP Server	switch(config)#**dhcpserver enable**
Dhcpserver disable	**G**	Disable DHCP Server	switch(config)#**no dhcpserver**
dhcpserver lowip [Low IP]	**G**	Configure low IP address for IP pool	switch(config)#**dhcpserver lowip 192.168.1.100**
dhcpserver highip [High IP]	**G**	Configure high IP address for IP pool	switch(config)#**dhcpserver highip 192.168.1.200**
dhcpserver subnetmask	**G**	Configure subnet	switch(config)#**dhcpserver**

[Subnet mask]		mask for DHCP clients	**subnetmask 255.255.255.0**
dhcpserver gateway [Gateway]	**G**	Configure gateway for DHCP clients	switch(config)#**dhcpserver gateway 192.168.1.254**
dhcpserver dnsip [DNS IP]	**G**	Configure DNS IP for DHCP clients	switch(config)#**dhcpserver dnsip 192.168.1.1**
dhcpserver leasetime [Hours]	**G**	Configure lease time (in hour)	switch(config)#**dhcpserver leasetime 1**
dhcpserver ipbinding [IP address]	**I**	Set static IP for DHCP clients by port	switch(config)#**interface fastEthernet 2** switch(config)#**dhcpserver ipbinding 192.168.1.1**
show dhcpserver configuration	**P**	Show configuration of DHCP server	switch#**show dhcpserver configuration**
show dhcpserver clients	**P**	Show client entries of DHCP server	switch#**show dhcpserver clients**
show dhcpserver ip-binding	**P**	Show IP-Binding information of DHCP server	switch#**show dhcpserver ip-binding**
no dhcpserver	**G**	Disable DHCP server function	switch(config)#**no dhcpserver**
security enable	**G**	Enable IP security function	switch(config)#**security enable**
security http	**G**	Enable IP security of HTTP server	switch(config)#**security http**
security telnet	**G**	Enable IP security of telnet server	switch(config)#**security telnet**
security ip [Index(1..10)] [IP Address]	**G**	Set the IP security list	switch(config)#**security ip 1 192.168.1.55**
show security	**P**	Show the information of IP security	switch#**show security**
no security	**G**	Disable IP security function	switch(config)#**no security**

no security http	**G**	Disable IP security of HTTP server	switch(config)#**no security http**
no security telnet	**G**	Disable IP security of telnet server	switch(config)#**no security telnet**

Port Commands Set

Netstar Commands	Level	Description	Example
interface fastEthernet [Portid]	**G**	Choose the port for modification.	switch(config)#**interface fastEthernet 2**
duplex [full | half]	**I**	Use the duplex configuration command to specify the duplex mode of operation for Fast Ethernet.	switch(config)#**interface fastEthernet 2** switch(config-if)#**duplex full**
speed [10|100|1000|auto]	**I**	Use the speed configuration command to specify the speed mode of operation for Fast Ethernet., the speed can't be set to 1000 if the port isn't a giga port..	switch(config)#**interface fastEthernet 2** switch(config-if)#**speed 100**
no flowcontrol	**I**	Disable flow control of interface	switch(config-if)#**no flowcontrol**
security enable	**I**	Enable security of interface	switch(config)#**interface fastEthernet 2** switch(config-if)#**security enable**
no security	**I**	Disable security of interface	switch(config)#**interface fastEthernet 2** switch(config-if)#**no security**

bandwidth type all	**I**	Set interface ingress limit frame type to 'accept all frame'	switch(config)#**interface fastEthernet 2** switch(config-if)#**bandwidth type all**
bandwidth type broadcast-multicast-flooded-unicast	**I**	Set interface ingress limit frame type to 'accept broadcast, multicast, and flooded unicast frame'	switch(config)#**interface fastEthernet 2** switch(config-if)#**bandwidth type broadcast-multicast-flooded-unicast**
bandwidth type broadcast-multicast	**I**	Set interface ingress limit frame type to 'accept broadcast and multicast frame'	switch(config)#**interface fastEthernet 2** switch(config-if)#**bandwidth type broadcast-multicast**
bandwidth type broadcast-only	**I**	Set interface ingress limit frame type to 'only accept broadcast frame'	switch(config)#**interface fastEthernet 2** switch(config-if)#**bandwidth type broadcast-only**
bandwidth in **[Value]**	**I**	Set interface input bandwidth. Rate Range is from 100 kbps to 102400 kbps or to 256000 kbps for giga ports, and zero means no limit.	switch(config)#**interface fastEthernet 2** switch(config-if)#**bandwidth in 100**
bandwidth out **[Value]**		Set interface output bandwidth. Rate Range is from 100 kbps to 102400 kbps or to 256000 kbps for giga ports, and zero means no limit.	switch(config)#**interface fastEthernet 2** switch(config-if)#**bandwidth out 100**

show bandwidth	**I**	Show interfaces bandwidth control	switch(config)#**interface fastEthernet 2** switch(config-if)#**show bandwidth**
state **[Enable | Disable]**	**I**	Use the state interface configuration command to specify the state mode of operation for Ethernet ports. Use the disable form of this command to disable the port.	switch(config)#**interface fastEthernet 2** switch(config-if)#**state Disable**
show interface configuration	**I**	show interface configuration status	switch(config)#**interface fastEthernet 2** switch(config-if)#**show interface configuration**
show interface status	**I**	show interface actual status	switch(config)#**interface fastEthernet 2** switch(config-if)#**show interface status**
show interface accounting	**I**	show interface statistic counter	switch(config)#**interface fastEthernet 2** switch(config-if)#**show interface accounting**
no accounting	**I**	Clear interface accounting information	switch(config)#**interface fastEthernet 2** switch(config-if)#**no accounting**

Trunk Commands Set

Netstar Commands	Level	Description	Example
aggregator priority **[1~65535]**	**G**	Set port group system priority	switch(config)#**aggregator priority 22**
aggregator activityport **[Group ID]**	**G**	Set activity port	switch(config)#**aggregator activityport 2**

[Port Numbers]			
aggregator group **[GroupID] [Port-list]** **lacp** **workp** **[Workport]**	**G**	Assign a trunk group with LACP active. [GroupID] :1~4 [Port-list]:Member port list, This parameter could be a port range(ex.1-4) or a port list separate by a comma(ex.2, 3, 6) [Workport]: The amount of work ports, this value could not be less than zero or be large than the amount of member ports.	switch(config)#**aggregator group 1 1-4 lacp workp 2** or switch(config)#**aggregator group 2 1,4,3 lacp workp 3**
aggregator group **[GroupID] [Port-list]** **nolacp**	**G**	Assign a static trunk group. [GroupID] :1~4 [Port-list]:Member port list, This parameter could be a port range(ex.1-4) or a port list separate by a comma(ex.2, 3, 6)	switch(config)#**aggregator group 1 2-4 nolacp** or switch(config)#**aggregator group 1 3,1,2 nolacp**
show aggregator	**P**	Show the information of trunk group	switch#**show aggregator 1** or switch#**show aggregator 2** or switch#**show aggregator 3**
no aggregator lacp **[GroupID]**	**G**	Disable the LACP function of trunk group	switch(config)#**no aggreator lacp 1**

no aggregator group [GroupID]	**G**	Remove a trunk group	switch(config)#**no aggreator group 2**

VLAN Commands Set

Netstar Commands	Level	Description	Example
vlan database	**P**	Enter VLAN configure mode	switch#**vlan database**
Vlanmode [portbase| 802.1q | gvrp]	**V**	To set switch VLAN mode.	switch(vlan)#**vlanmode portbase** or switch(vlan)#**vlanmode 802.1q** or switch(vlan)#**vlanmode gvrp**
no vlan	**V**	No VLAN	Switch(vlan)#**no vlan**
Ported based VLAN configuration			
vlan port-based grpname [Group Name] **grpid** [GroupID] **port** [PortNumbers]	**V**	Add new port based VALN	switch(vlan)#**vlan port-based grpname test grpid 2 port 2-4** or switch(vlan)#**vlan port-based grpname test grpid 2 port 2,3,4**
show vlan [GroupID] or **show vlan**	**V**	Show VLAN information	switch(vlan)#**show vlan 23**
no vlan group [GroupID]	**V**	Delete port base group ID	switch(vlan)#**no vlan group 2**
IEEE 802.1Q VLAN			
vlan 8021q name [GroupName] **vid** [VID]	**V**	Change the name of VLAN group, if the group didn't exist, this command can't be applied.	switch(vlan)#**vlan 8021q name test vid 22**
vlan 8021q port [PortNumber] **access-link untag**	**V**	Assign a access link for VLAN by port, if the	switch(vlan)#**vlan 8021q port 3 access-link untag 33**

[UntaggedVID]		port belong to a trunk group, this command can't be applied.	
vlan 8021q port [PortNumber] trunk-link tag [TaggedVID List]	**V**	Assign a trunk link for VLAN by port, if the port belong to a trunk group, this command can't be applied.	switch(vlan)#**vlan 8021q port 3 trunk-link tag 2,3,6,99** or switch(vlan)#**vlan 8021q port 3 trunk-link tag 3-20**
vlan 8021q port [PortNumber] hybrid-link untag [UntaggedVID] tag [TaggedVID List]	**V**	Assign a hybrid link for VLAN by port, if the port belong to a trunk group, this command can't be applied.	switch(vlan)#**vlan 8021q port 3 hybrid-link untag 4 tag 3,6,8** or switch(vlan)#**vlan 8021q port 3 hybrid-link untag 5 tag 6-8**
vlan 8021q trunk [PortNumber] access-link untag [UntaggedVID]	**V**	Assign a access link for VLAN by trunk group	switch(vlan)#**vlan 8021q trunk 3 access-link untag 33**
vlan 8021q trunk [PortNumber] trunk-link tag [TaggedVID List]	**V**	Assign a trunk link for VLAN by trunk group	switch(vlan)#**vlan 8021q trunk 3 trunk-link tag 2,3,6,99** or switch(vlan)#**vlan 8021q trunk 3 trunk-link tag 3-20**
vlan 8021q trunk [PortNumber] hybrid-link untag [UntaggedVID] tag [TaggedVID List]	**V**	Assign a hybrid link for VLAN by trunk group	switch(vlan)#**vlan 8021q trunk 3 hybrid-link untag 4 tag 3,6,8** or switch(vlan)#**vlan 8021q trunk 3 hybrid-link untag 5 tag 6-8**
show vlan [GroupID] or **show vlan**	**V**	Show VLAN information	switch(vlan)#**show vlan 23**
no vlan group [GroupID]	**V**	Delete port base group ID	switch(vlan)#**no vlan group 2**

Spanning Tree Commands Set

Netstar Commands	Level	Description	Example

spanning-tree enable	**G**	Enable spanning tree	switch(config)#**spanning-tree enable**
spanning-tree priority [0~61440]	**G**	Configure spanning tree priority parameter	switch(config)#**spanning-tree priority 32767**
spanning-tree max-age [seconds]	**G**	Use the spanning-tree max-age global configuration command to change the interval between messages the spanning tree receives from the root switch. If a switch does not receive a bridge protocol data unit (BPDU) message from the root switch within this interval, it recomputed the Spanning Tree Protocol (STP) topology.	switch(config)#**spanning-tree max-age 15**
spanning-tree hello-time [seconds]	**G**	Use the spanning-tree hello-time global configuration command to specify the interval between hello bridge protocol data units (BPDUs).	switch(config)#**spanning-tree hello-time 3**
spanning-tree forward-time [seconds]	**G**	Use the spanning-tree forward-time global configuration command to set the	switch(config)#**spanning-tree forward-time 20**

		forwarding-time for the specified spanning-tree instances. The forwarding time determines how long each of the listening and learning states last before the port begins forwarding.	
stp-path-cost **[1~200000000]**	**I**	Use the spanning-tree cost interface configuration command to set the path cost for Spanning Tree Protocol (STP) calculations. In the event of a loop, spanning tree considers the path cost when selecting an interface to place into the forwarding state.	switch(config)#**interface fastEthernet 2** switch(config-if)#**stp-path-cost 20**
stp-path-priority [Port Priority]	**I**	Use the spanning-tree port-priority interface configuration command to configure a port priority that is used when two switches tie for position as the root switch.	switch(config)#**interface fastEthernet 2** switch(config-if)#**stp-path-priority 128**

stp-admin-p2p [Auto|True|False]	**I**	Admin P2P of STP priority on this interface.	switch(config)#**interface fastEthernet 2** switch(config-if)#**stp-admin-p2p Auto**
stp-admin-edge [True|False]	**I**	Admin Edge of STP priority on this interface.	switch(config)#**interface fastEthernet 2** switch(config-if)#**stp-admin-edge True**
stp-admin-non-stp [True|False]	**I**	Admin NonSTP of STP priority on this interface.	switch(config)#**interface fastEthernet 2** switch(config-if)#**stp-admin-non-stp False**
show spanning-tree	**E**	Displays a summary of the spanning-tree states.	switch>**show spanning-tree**
no spanning-tree	**G**	Disable spanning-tree.	switch(config)#**no spanning-tree**

QOS Commands Set

Netstar Commands	Level	Description	Example
qos policy [weighted-fair|strict]	**G**	Select QOS policy scheduling	switch(config)#**qos policy weighted-fair**
qos prioritytype [port-based|cos-only|tos-only|cos-first|tos-first]	**G**	Setting of QOS priority type	switch(config)#**qos prioritytype**
qos priority portbased [Port] [lowest|low|middle|high]	**G**	Configure Port-based Priority	switch(config)#**qos priority portbased 1 low**
qos priority cos [Priority][lowest|low|middle|high]	**G**	Configure COS Priority	switch(config)#**qos priority cos 0 middle**
qos priority tos [Priority][lowest|low|middle|high]	**G**	Configure TOS Priority	switch(config)#**qos priority tos 3 high**
show qos	**P**	Displays the	Switch#**show qos**

		information of QoS configuration	
no qos	**G**	Disable QoS function	switch(config)#**no qos**

IGMP Commands Set

Netstar Commands	Level	Description	Example
igmp enable	**G**	Enable IGMP snooping function	switch(config)#**igmp enable**
lgmp-query auto	**G**	Set IGMP query to auto mode	switch(config)#**lgmp-query auto**
lgmp-query force	**G**	Set IGMP query to force mode	switch(config)#**lgmp-query force**
show igmp configuration	**P**	Displays the details of an IGMP configuration.	switch#**show igmp configuration**
show igmp multi	**P**	Displays the details of an IGMP snooping entries.	switch#**show igmp multi**
no igmp	**G**	Disable IGMP snooping function	switch(config)#**no igmp**
no igmp-query	**G**	Disable IGMP query	switch#**no igmp-query**

Mac / Filter Table Commands Set

Netstar Commands	Level	Description	Example
mac-address-table static hwaddr [MAC]	**I**	Configure MAC address table of interface (static).	switch(config)#**interface fastEthernet 2** switch(config-if)#**mac-address-table static hwaddr 000012345678**
mac-address-table filter hwaddr [MAC]	**G**	Configure MAC address table(filter)	switch(config)#**mac-address-table filter hwaddr 000012348678**

show mac-address-table	**P**	Show all MAC address table	switch#**show mac-address-table**
show mac-address-table static	**P**	Show static MAC address table	switch#**show mac-address-table static**
show mac-address-table filter	**P**	Show filter MAC address table.	switch#**show mac-address-table filter**
no mac-address-table static hwaddr [MAC]	**I**	Remove an entry of MAC address table of interface (static)	switch(config)#**interface fastEthernet 2** switch(config-if)#**no mac-address-table static hwaddr 000012345678**
no mac-address-table filter hwaddr [MAC]	**G**	Remove an entry of MAC address table (filter)	switch(config)#**no mac-address-table filter hwaddr 000012348678**
no mac-address-table	**G**	Remove dynamic entry of MAC address table	switch(config)#**no mac-address-table**

SNMP Commands Set

Netstar Commands	Level	Description	Example
snmp system-name [System Name]	**G**	Set SNMP agent system name	switch(config)#**snmp system-name l2switch**
snmp system-location [System Location]	**G**	Set SNMP agent system location	switch(config)#**snmp system-location lab**
snmp system-contact [System Contact]	**G**	Set SNMP agent system contact	switch(config)#**snmp system-contact where**
snmp agent-mode [v1v2c|v3|v1v2cv3]	**G**	Select the agent mode of SNMP	switch(config)#**snmp agent-mode v1v2cv3**
snmp community-strings [Community] right [RO/RW]	**G**	Add SNMP community string.	switch(config)#**snmp community-strings public right rw**
snmp-server host	**G**	Configure SNMP	switch(config)#**snmp-server host**

[IP address] community [Community-string] trap-version [v1|v2c]		server host information and community string	**192.168.1.50 community public trap-version v1 (remove)** Switch(config)#**no snmp-server host 192.168.1.50**
snmpv3 context-name [Context Name]	**G**	Configure the context name	switch(config)#**snmpv3 context-name Test**
snmpv3 user [User Name] group [Group Name] password [Authentication Password] [Privacy Password]	**G**	Configure the userprofile for SNMPV3 agent. Privacy password could be empty.	switch(config)#**snmpv3 user test01 group G1 password AuthPW PrivPW**
snmpv3 access context-name [Context Name] group [Group Name] security-level [NoAuthNoPriv|AuthNoPriv|AuthPriv] match-rule [Exact|Prifix] views [Read View Name] [Write View Name] [Notify View Name]	**G**	Configure the access table of SNMPV3 agent	switch(config)#**snmpv3 access context-name Test group G1 security-level AuthPriv match-rule Exact views V1 V1 V1**
snmpv3 mibview view [View Name] type [Excluded|Included] sub-oid	**G**	Configure the mibview table of SNMPV3 agent	switch(config)#**snmpv3 mibview view V1 type Excluded sub-oid 1.3.6.1**

[OID]			
show snmp	**P**	Show SNMP configuration	switch#**show snmp**
no snmp community-strings [Community]	**G**	Remove the specified community.	switch(config)#**no snmp community-strings public**
no snmp-server host [Host-address]	**G**	Remove the SNMP server host.	switch(config)#**no snmp-server host 192.168.1.50**
no snmpv3 user [User Name]	**G**	Remove specified user of SNMPv3 agent.	switch(config)#**no snmpv3 user Test**
no snmpv3 access context-name [Context Name] group [Group Name] security-level [NoAuthNoPriv|AuthNoPriv|AuthPriv] match-rule [Exact|Prifix] views [Read View Name] [Write View Name] [Notify View Name]	**G**	Remove specified access table of SNMPv3 agent.	switch(config)#**no snmpv3 access context-name Test group G1 security-level AuthPriv match-rule Exact views V1 V1 V1**
no snmpv3 mibview view [View Name] type [Excluded|Included] sub-oid [OID]	**G**	Remove specified mibview table of SNMPV3 agent.	switch(config)#**no snmpv3 mibview view V1 type Excluded sub-oid 1.3.6.1**

Port Mirroring Commands Set

Netstar Commands	Level	Description	Example
monitor rx	G	Set RX destination port of monitor function	switch(config)#**monitor rx**
monitor tx	G	Set TX destination port of monitor function	switch(config)#**monitor tx**
show monitor	P	Show port monitor information	switch#**show monitor**
monitor **[RX|TX|Both]**	I	Configure source port of monitor function	switch(config)#**interface fastEthernet 2** switch(config-if)#**monitor RX**
show monitor	I	Show port monitor information	switch(config)#**interface fastEthernet 2** switch(config-if)#**show monitor**
no monitor	I	Disable source port of monitor function	switch(config)#**interface fastEthernet 2** switch(config-if)#**no monitor**

802.1x Commands Set

Netstar Commands	Level	Description	Example
8021x enable	G	Use the 802.1x global configuration command to enable 802.1x protocols.	switch(config)# **8021x enable**
8021x system radiusip **[IP address]**	G	Use the 802.1x system radius IP global configuration command to change the radius server IP.	switch(config)# **8021x system radiusip 192.168.1.1**
8021x system serverport	G	Use the 802.1x	switch(config)# **8021x system**

[port ID]		system server port global configuration command to change the radius server port	**serverport 1812**
8021x system accountport [port ID]	**G**	Use the 802.1x system account port global configuration command to change the accounting port	switch(config)# **8021x system accountport 1813**
8021x system sharedkey [ID]	**G**	Use the 802.1x system share key global configuration command to change the shared key value.	switch(config)# **8021x system sharedkey 123456**
8021x system nasid [words]	**G**	Use the 802.1x system nasid global configuration command to change the NAS ID	switch(config)# **8021x system nasid test1**
8021x misc quietperiod [sec.]	**G**	Use the 802.1x misc quiet period global configuration command to specify the quiet period value of the switch.	switch(config)# **8021x misc quietperiod 10**
8021x misc txperiod [sec.]	**G**	Use the 802.1x misc TX period global configuration command to set the TX period.	switch(config)# **8021x misc txperiod 5**
8021x misc supptimeout [sec.]	**G**	Use the 802.1x misc supp timeout global configuration	switch(config)# **8021x misc supptimeout 20**

		command to set the supplicant timeout.	
8021x misc servertimeout [sec.]	**G**	Use the 802.1x misc server timeout global configuration command to set the server timeout.	switch(config)#**8021x misc servertimeout 20**
8021x misc maxrequest [number]	**G**	Use the 802.1x misc max request global configuration command to set the MAX requests.	switch(config)# **8021x misc maxrequest 3**
8021x misc reauthperiod [sec.]	**G**	Use the 802.1x misc reauth period global configuration command to set the reauth period.	switch(config)# **8021x misc reauthperiod 3000**
8021x portstate [disable | reject | accept | authorize]	**I**	Use the 802.1x port state interface configuration command to set the state of the selected port.	switch(config)#**interface fastethernet 3** switch(config-if)#**8021x portstate accept**
show 8021x	**E**	Displays a summary of the 802.1x properties and also the port sates.	switch>**show 8021x**
no 8021x	**G**	Disable 802.1x function	switch(config)#**no 8021x**

TFTP Commands Set

Netstar Commands	Level	Description	Defaults Example

backup flash:backup_cfg	**G**	Save configuration to TFTP and need to specify the IP of TFTP server and the file name of image.	switch(config)#**backup flash:backup_cfg**
restore flash:restore_cfg	**G**	Get configuration from TFTP server and need to specify the IP of TFTP server and the file name of image.	switch(config)#**restore flash:restore_cfg**
upgrade flash:upgrade_fw	**G**	Upgrade firmware by TFTP and need to specify the IP of TFTP server and the file name of image.	switch(config)#**upgrade flash:upgrade_fw**

SystemLog, SMTP and Event Commands Set

Netstar Commands	Level	Description	Example
systemlog ip [IP address]	**G**	Set System log server IP address.	switch(config)# **systemlog ip 192.168.1.100**
systemlog mode [client|server|both]	**G**	Specified the log mode	switch(config)# **systemlog mode both**
show systemlog	**E**	Displays system log.	Switch>**show systemlog**
show systemlog	**P**	Show system log client & server information	switch#**show systemlog**
no systemlog	**G**	Disable systemlog functon	switch(config)#**no systemlog**
smtp enable	**G**	Enable SMTP function	switch(config)#**smtp enable**
smtp serverip [IP address]	**G**	Configure SMTP server IP	switch(config)#**smtp serverip 192.168.1.5**
smtp authentication	**G**	Enable SMTP authentication	switch(config)#**smtp authentication**

smtp account [account]	**G**	Configure authentication account	switch(config)#**smtp account User**
smtp password [password]	**G**	Configure authentication password	switch(config)#**smtp password**
smtp rcptemail [Index] [Email address]	**G**	Configure Rcpt e-mail Address	switch(config)#**smtp rcptemail 1 Alert@test.com**
show smtp	**P**	Show the information of SMTP	switch#**show smtp**
no smtp	**G**	Disable SMTP function	switch(config)#**no smtp**
event device-cold-start [Systemlog|SMTP|Both]	**G**	Set cold start event type	switch(config)#**event device-cold-start both**
event authentication-failure [Systemlog|SMTP|Both]	**G**	Set Authentication failure event type	switch(config)#**event authentication-failure both**
event ring-topology-change [Systemlog|SMTP|Both]	**G**	Set X-ring topology changed event type	switch(config)#**event ring-topology-change both**
event systemlog [Link-UP|Link-Down|Both]	**I**	Set port event for system log	switch(config)#**interface fastethernet 3** switch(config-if)#**event systemlog both**
event smtp [Link-UP|Link-Down|Both]	**I**	Set port event for SMTP	switch(config)#**interface fastethernet 3** switch(config-if)#**event smtp both**
show event	**P**	Show event selection	switch#**show event**
no event device-cold-start	**G**	Disable cold start event type	switch(config)#**no event device-cold-start**
no event authentication-failure	**G**	Disable Authentication failure event type	switch(config)#**no event authentication-failure**
no event ring-topology-change	**G**	Disable X-ring topology changed	switch(config)#**no event ring-topology-change**

		event type	
no event systemlog	**I**	Disable port event for system log	switch(config)#**interface fastethernet 3** switch(config-if)#**no event systemlog**
no event smtp	**I**	Disable port event for SMTP	switch(config)#**interface fastethernet 3** switch(config-if)#**no event smtp**
show systemlog	**P**	Show system log client & server information	switch#**show systemlog**

SNTP Commands Set

Netstar Commands	Level	Description	Example
sntp enable	**G**	Enable SNTP function	switch(config)#**sntp enable**
sntp daylight	**G**	Enable daylight saving time, if SNTP function is inactive, this command can't be applied.	switch(config)#**sntp daylight**
sntp daylight-period **[Start time] [End time]**	**G**	Set period of daylight saving time, if SNTP function is inactive, this command can't be applied. Parameter format: [yyyymmdd-hh:mm]	switch(config)# **sntp daylight-period 20060101-01:01 20060202-01-01**
sntp daylight-offset **[Minute]**	**G**	Set offset of daylight saving time, if SNTP function is inactive, this command can't be applied.	switch(config)#**sntp daylight-offset 3**

sntp ip **[IP]**	**G**	Set SNTP server IP, if SNTP function is inactive, this command can't be applied.	switch(config)#**sntp ip 192.169.1.1**
sntp timezone **[Timezone]**	**G**	Set timezone index, use 'show sntp timzezone' command to get more information of index number	switch(config)#**sntp timezone 22**
show sntp	**P**	Show SNTP information	switch#**show sntp**
show sntp timezone	**P**	Show index number of time zone list	switch#**show sntp timezone**
no sntp	**G**	Disable SNTP function	switch(config)#**no sntp**
no sntp daylight	**G**	Disable daylight saving time	switch(config)#**no sntp daylight**

X-ring Commands Set

Netstar Commands	Level	Description	Example
ring enable	**G**	Enable X-ring	switch(config)#**ring enable**
ring master	**G**	Enable ring master	switch(config)#**ring master**
ring couplering	**G**	Enable couple ring	switch(config)#**ring couplering**
ring dualhoming	**G**	Enable dual homing	switch(config)#**ring dualhoming**
ring ringport **[1st Ring Port] [2nd Ring Port]**	**G**	Configure 1st/2nd Ring Port	switch(config)#**ring ringport 7 8**
ring couplingport **[Coupling Port]**	**G**	Configure Coupling Port	switch(config)#**ring couplingport 1**
ring controlport **[Control Port]**	**G**	Configure Control Port	switch(config)#**ring controlport 2**

ring homingport [Dual Homing Port]	**G**	Configure Dual Homing Port	switch(config)#**ring homingport 3**
show ring	**P**	Show the information of X - Ring	switch#**show ring**
no ring	**G**	Disable X-ring	switch(config)#**no ring**
no ring master	**G**	Disable ring master	switch(config)# **no ring master**
no ring couplering	**G**	Disable couple ring	switch(config)# **no ring couplering**
no ring dualhoming	**G**	Disable dual homing	switch(config)# **no ring dualhoming**

Web-Based Management

This section introduces the configuration and functions of the Web-Based management.

About Web-based Management

On the CPU board of the switch there is an embedded HTML web site residing in flash memory. This offers advanced management features and allow users to manage the switch from anywhere on the network through a standard browser such as Microsoft Internet Explorer.

The Web-Based Management supports Internet Explorer 6.0 or later version. It utilizes Java Applets for reducing network bandwidth consumption, enhancing access speed and presenting an easy viewing screen.

Preparing for Web Management

Before using web management, install the industrial switch on the network and make sure that any one of the PCs on the network can connect with the industrial switch through the web browser. The industrial switch default value of IP, subnet mask, username and password are as follows:

- IP Address: **192.168.1.77**
- Subnet Mask: **255.255.255.0**
- Default Gateway: **192.168.1.254**
- User Name: **root**
- Password: **root**

System Login

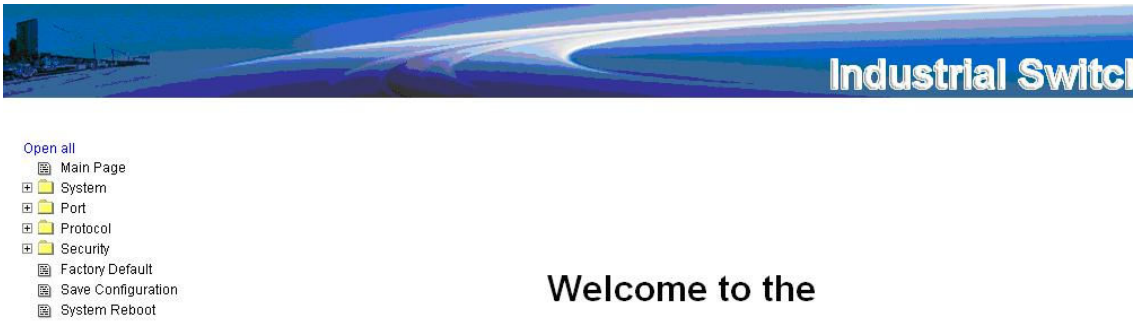
1. Launch the Internet Explorer on the PC
2. Key in “http:// “+” the IP address of the switch”, and then Press “**Enter**”.

3. The login screen will appear right after
4. Key in the user name and password. The default user name and password are the same as “**root**”
5. Press “**Enter**” or ”**OK**”, and then the home screen of the Web-based management appears as below:

Login screen

Main Page

The home page of the Web-based screen mainly consists of a treeview control item. For more details about each function, please click the '+' symbol of each node to expand the tree structure.

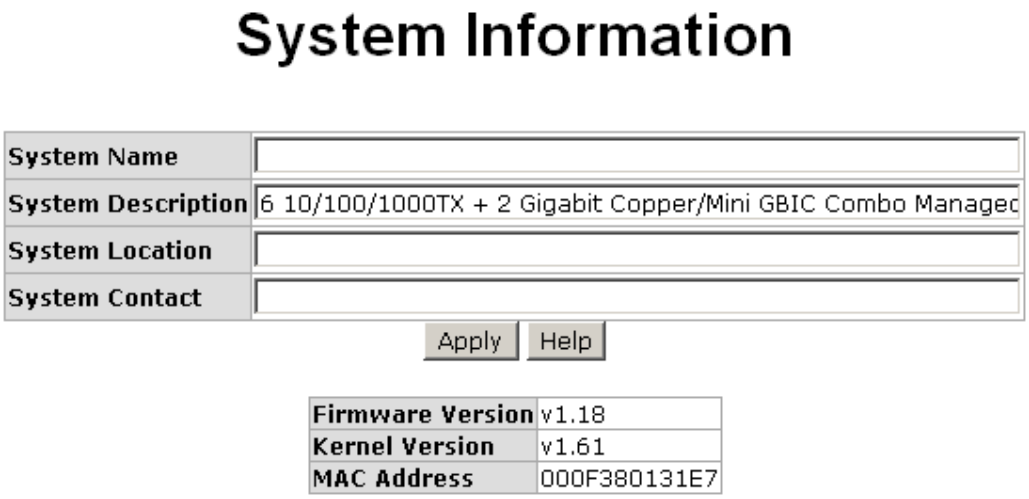


Main interface

System Information

Assign the system name, location and view the system information.

- **System Name:** Assign the name of switch. The maximum length is 64 bytes.
- **System Description:** Displays the description of switch. This column is read only; cannot be modified.
- **System Location:** Assign the switch physical location. The maximum length is 64 bytes.
- **System Contact:** Enter the name of contact person or organization.
- **Firmware Version:** Displays the switch's firmware version.
- **Kernel Version:** Displays the kernel software version.
- **MAC Address:** Displays the unique hardware address assigned by manufacturer (default).

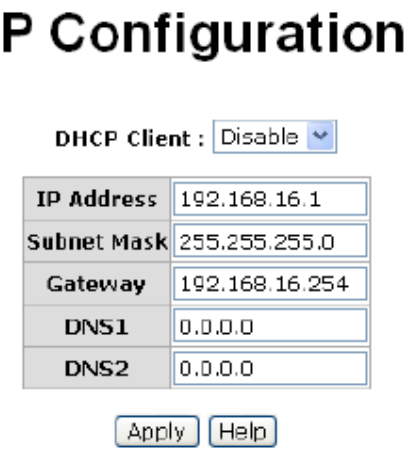


System information interface

IP Configuration

User can configure the IP Settings and DHCP client function

- **DHCP Client:** Enable or disable the DHCP client function. When DHCP client function is enabled, the industrial switch will be assigned an IP address from the network DHCP server. The default IP address will be replaced with an IP address which is assigned by the DHCP server. After user click "**Apply**" button, a pop-up dialog show up. It is to inform the user that when the DHCP client is enabled, the current IP will lose and user should find the new IP on the DHCP server.
- **IP Address:** Assign the IP address that the network is using. If DHCP client function is enabled, then user needn't assign the IP address manually. Instead, the network DHCP server will assign the IP address for the industrial switch and display it in this column. The default IP is 192.168.1.77
- **Subnet Mask:** Assign the subnet mask of the IP address. If DHCP client function is enabled, and then user needn't assign the subnet mask manually
- **Gateway:** Assign the network gateway for the industrial switch. The default gateway is 192.168.1.254
- **DNS1:** Assign the primary DNS IP address.
- **DNS2:** Assign the secondary DNS IP address.
- And then, click Apply

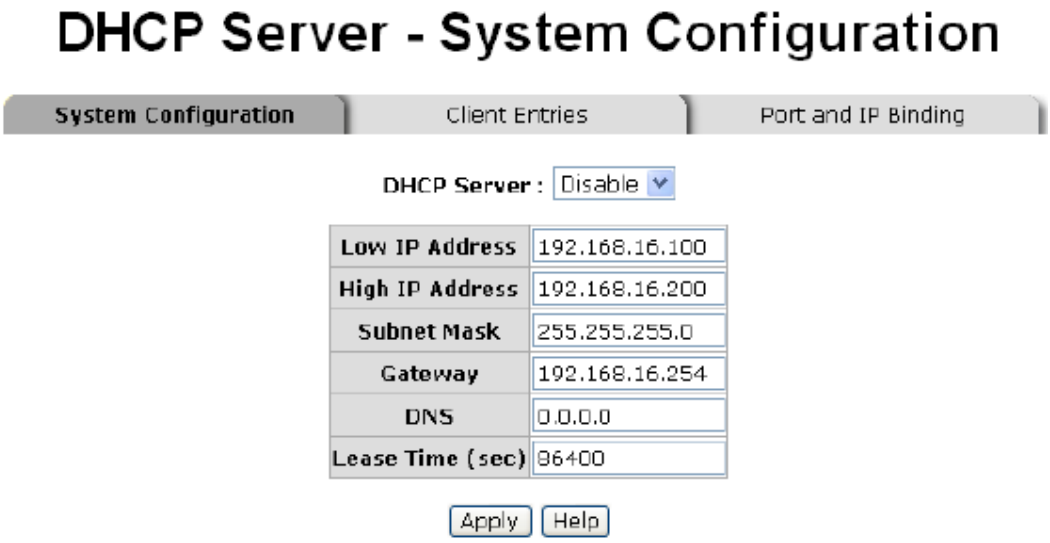


IP configuration interface

DHCP Server—System configuration

The system provides the DHCP server function. Enable the DHCP server function, the switch system will be a DHCP server.

- **DHCP Server:** Enable or Disable the DHCP Server function. Enable – the switch will be the DHCP server on your local network.
- **Low IP Address:** the dynamic IP assign range. Low IP address is the beginning of the dynamic IP assigns range. For example: dynamic IP assign range is from 192.168.1.100 ~ 192.168.1.200. 192.168.1.100 will be the Low IP address.
- **High IP Address:** the dynamic IP assign range. High IP address is the end of the dynamic IP assigns range. For example, dynamic IP assign range is from 192.168.1.100 ~ 192.168.1.200. Therefore, 192.168.1.200 is the High IP address.
- **Subnet Mask:** The dynamic IP assign range subnet mask.
- **Gateway:** The gateway in your network.
- **DNS:** Domain Name Server IP Address in your network.
- **Lease Time (sec):** It is the time period that system will reset the dynamic IP assignment to ensure the dynamic IP won't have been occupied for a long time; otherwise the server won't know that the dynamic IP is idle.
- And then, click Apply



DHCP Server Configuration interface

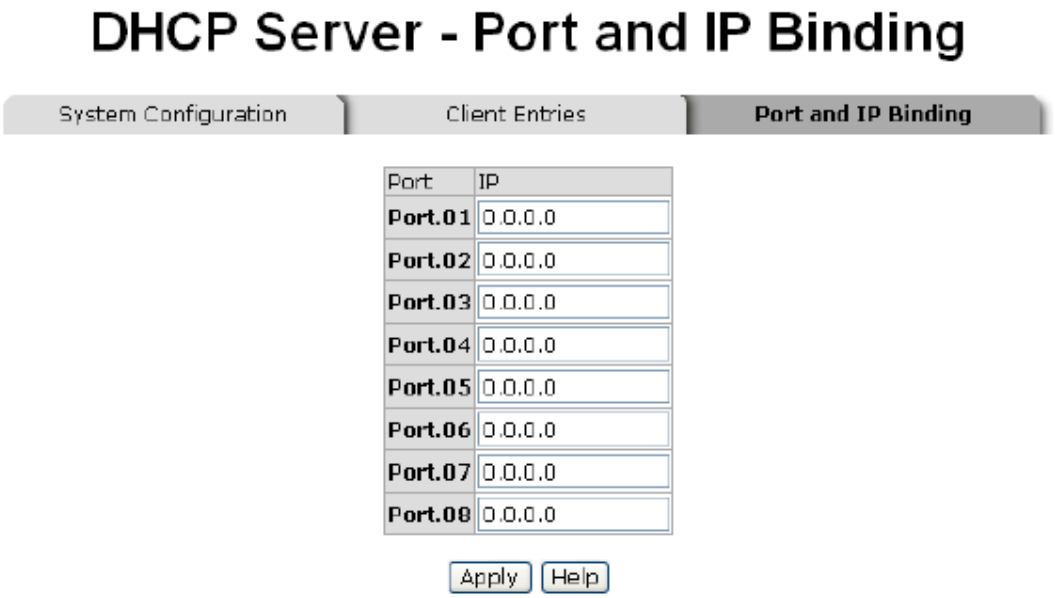
DHCP Client—Client Entries

When the DHCP server function is active, the system will collect the DHCP client information and display it here.

DHCP Client Entries interface

DHCP Server—Port and IP Bindings

You can assign the specific IP address that is the IP in the dynamic IP assign range to the specific port. When the device is connected to the port and asks for dynamic IP assigning, the system will assign the IP address that has been assigned to the connected device.

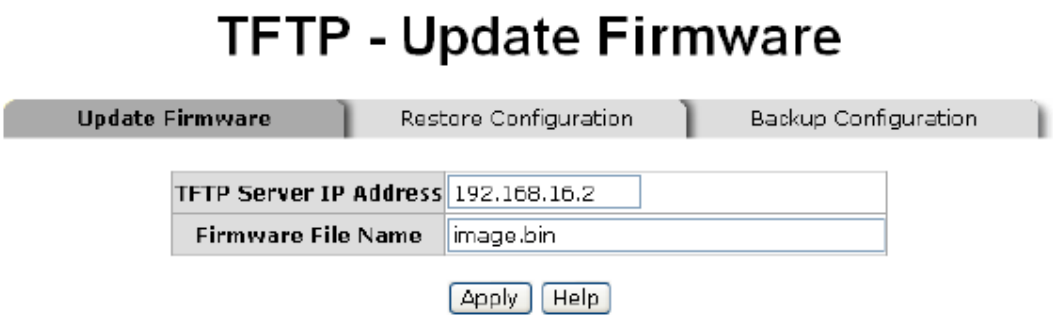


Port and IP Bindings interface

TFTP—Update Firmware

TFTP allows the user to update the switch firmware remotely, via the network. Before updating, make sure you have your TFTP server ready and the firmware image is on the TFTP server.

1. **TFTP Server IP Address:** Fill in your TFTP server IP.
2. **Firmware File Name:** the name of firmware image.
3. Click Apply.



Update Firmware interface

TFTP—Restore Configuration

You can restore the switch configuration from the TFTP server, but you must put the image file on TFTP server first. The switch will then download the flash image.

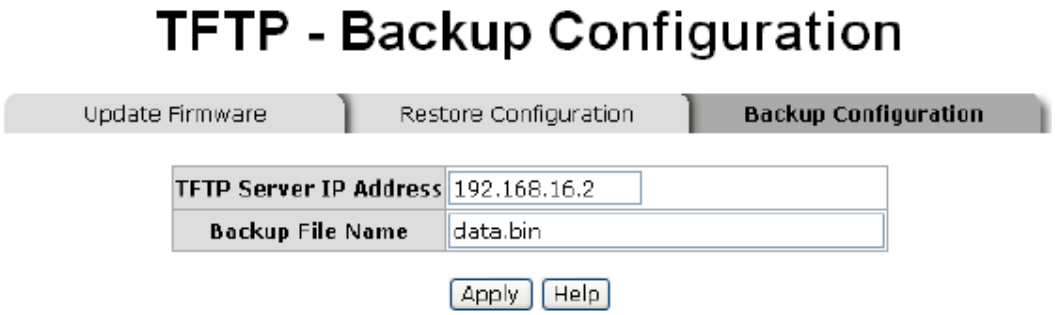
1. **TFTP Server IP Address:** Fill in the TFTP server IP.
2. **Restore File Name:** Fill in the correct restore file name.
3. Click Apply.

Restore Configuration interface

TFTP—Backup Configuration

You can save the current switch configuration from the switch to TFTP server, then go to the TFTP restore configuration page to restore the switch configuration.

1. **TFTP Server IP Address:** Fill in the TFTP server IP.
2. **Backup File Name:** Fill the file name.
3. Click Apply.

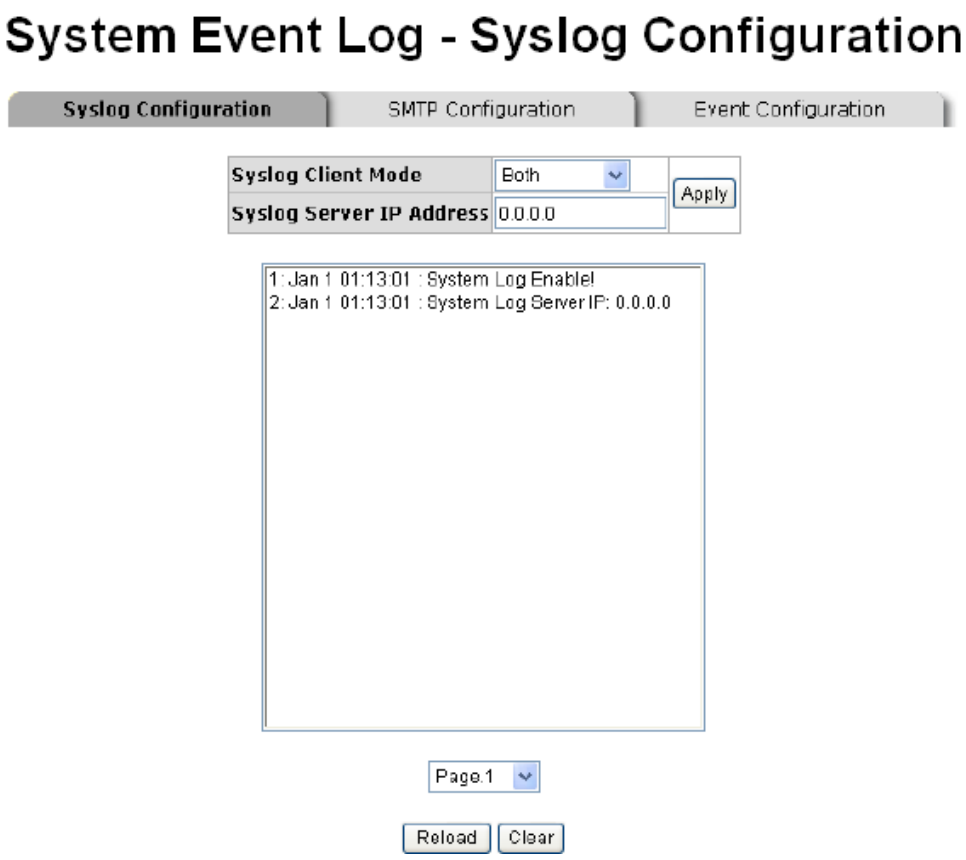


Backup Configuration interface

System Event Log—Syslog Configuration

Configure the system events that you want to record and the system log server IP.

1. **Syslog Client Mode:** Select the system log mode – client only, server only, or both S/C.
2. **System Log Server IP Address:** Assigned the system log server IP.
3. Click Reload to refresh the events log.
4. Click Clear to clear all current events log.
5. After configuring, click Apply.

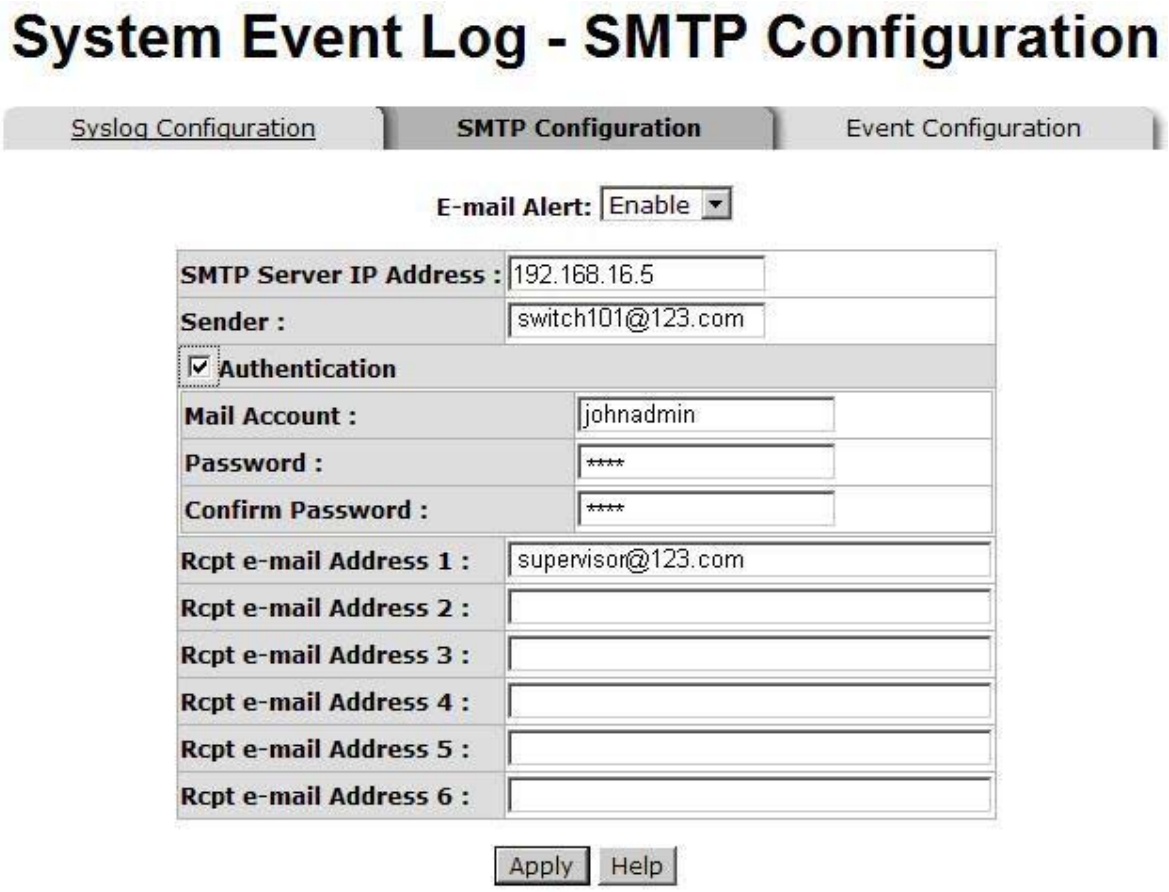


Syslog Configuration interface

System Event Log—SMTP Configuration

You can set up the mail server IP, mail account, account password, and forwarded email account for receiving the event alert.

1. **Email Alert:** enable or disable the email alert function.
2. **SMTP Server IP:** set up the mail server IP address (when **Email Alert** enabled, this function will then be available).
3. **Sender:** key in a complete email address, e.g. switch101@123.com, to identify where the event log comes from.
4. **Authentication:** mark the check box to enable and configure the email account and password for authentication (when **Email Alert** enabled, this function will then be available).
5. **Mail Account:** set up the email account, e.g. johnadmin, to receive the alert. It must be an existing email account on the mail server, which you had set up in **SMTP Server IP Address** column.
6. **Password:** The email account password.
7. **Confirm Password:** reconfirm the password.
8. **Rcpt e-mail Address 1 ~ 6:** you can assign up to 6 e-mail accounts also to receive the alert.
9. Click Apply.

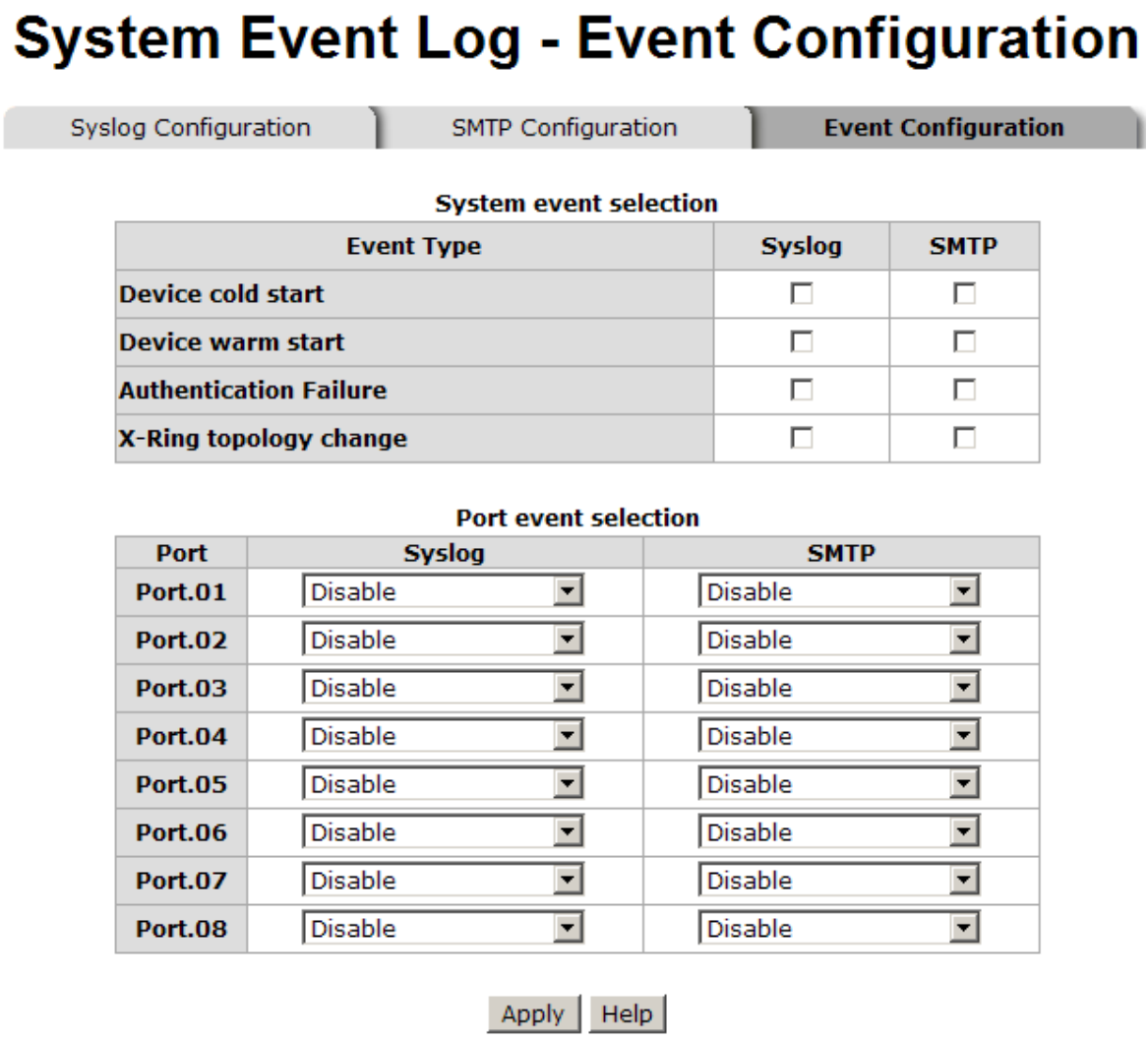


SMTP Configuration interface

System Event Log—Event Configuration

You can select the system log events and SMTP events. When selected events occur, the system will send out the log information. Also, per port log and SMTP events can be selected. After configuring, Click Apply.

- **System event selection:** 4 selections – Device cold start, Device warm start, SNMP Authentication Failure, and X-ring topology change. Mark the checkbox to select the event. When selected events occur, the system will issue the logs.
  - **Device cold start:** When the device executes cold start action, the system will issue a log event.
  - **Device warm start:** When the device executes warm start, the system will issue a log event.
  - **Authentication Failure:** When the SNMP authentication fails, the system will issue a log event.
  - **X-ring topology change:** When the X-ring topology has changed, the system will issue a log event.
- **Port event selection:** Select the per port events and per port SMTP events. It has 3 selections – Link UP, Link Down, and Link UP & Link Down. Disable means no event is selected.
  - **Link UP:** the system will issue a log message when port connection is up only.
  - **Link Down:** the system will issue a log message when port connection is down only.
  - **Link UP & Link Down:** the system will issue a log message when port connection is up and down.

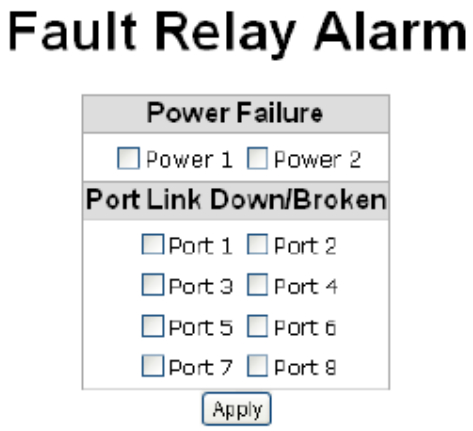


Event Configuration interface

Fault Relay Alarm

The Fault Relay Alarm function provides the mechanism for warning when power or port faults are detected. There is a set of relay contacts in the switch, and the contacts are closed when either no fault alarms are configured, or the system is normal. With the check boxes unchecked, the system won't change the status of the relay when a fault occurs. Please see the segment of '**Wiring the Fault Alarm Contact**' for reference. With both power input 1 and power input 2 installed and the check boxes of power 1/power 2 ticked, the FAULT LED indicator will then be possible to light up when any one of the power fault occurs. As for the Port Link Down/Broken detection, the FAULT LED indicator will light up when the port fault occurs.

- **Power Failure:** Tick the check box to enable the function of lighting up the **FAULT** LED on the panel when power fails.
- **Port Link Down/Broken:** Tick the check box to enable the function of lighting up **FAULT** LED on the panel when Ports' states are link down or broken.



Fault Relay Alarm interface

SNTP Configuration

You can configure the SNTP (Simple Network Time Protocol) settings. The SNTP allows you to synchronize switch clocks via the Internet.

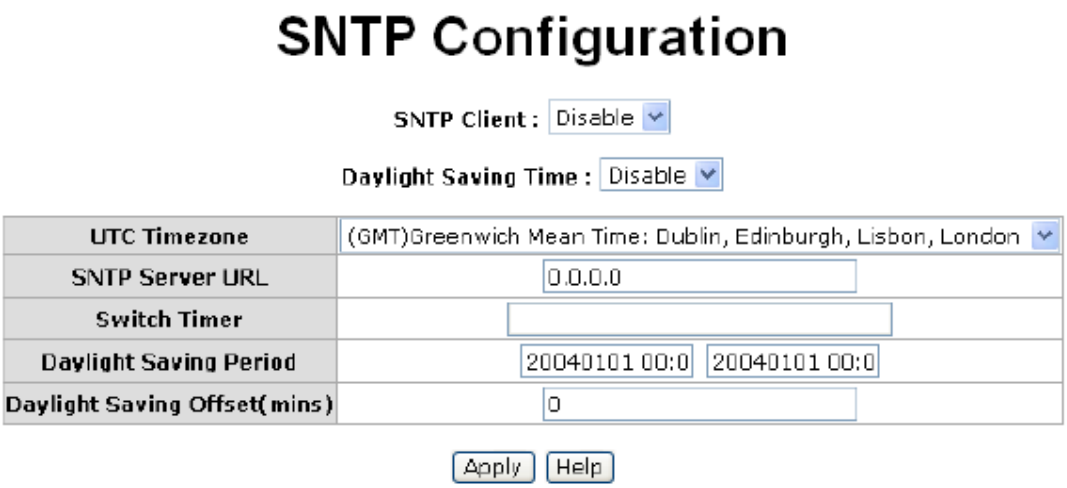
1. **SNTP Client:** Enable or disable SNTP function to get the time from the SNTP server.
2. **Daylight Saving Time:** Enable or disable daylight saving time function. When daylight saving time is enabled, you need to configure the daylight saving time period.
3. **UTC Timezone:** Set the switch location time zone. The following table lists the different location time zones for your reference.

Local Time Zone	Conversion from UTC	Time at 12:00 UTC
November Time Zone	- 1 hour	11am
Oscar Time Zone	-2 hours	10 am
ADT - Atlantic Daylight	-3 hours	9 am
AST - Atlantic Standard EDT - Eastern Daylight	-4 hours	8 am
EST - Eastern Standard CDT - Central Daylight	-5 hours	7 am
CST - Central Standard MDT - Mountain Daylight	-6 hours	6 am
MST - Mountain Standard PDT - Pacific Daylight	-7 hours	5 am
PST - Pacific Standard ADT - Alaskan Daylight	-8 hours	4 am
ALA - Alaskan Standard	-9 hours	3 am

HAW - Hawaiian Standard	-10 hours	2 am
Nome, Alaska	-11 hours	1 am
CET - Central European FWT - French Winter MET - Middle European MEWT - Middle European Winter SWT - Swedish Winter	+1 hour	1 pm
EET - Eastern European, USSR Zone 1	+2 hours	2 pm
BT - Baghdad, USSR Zone 2	+3 hours	3 pm
ZP4 - USSR Zone 3	+4 hours	4 pm
ZP5 - USSR Zone 4	+5 hours	5 pm
ZP6 - USSR Zone 5	+6 hours	6 pm
WAST - West Australian Standard	+7 hours	7 pm
CCT - China Coast, USSR Zone 7	+8 hours	8 pm
JST - Japan Standard, USSR Zone 8	+9 hours	9 pm
EAST - East Australian Standard GST Guam Standard, USSR Zone 9	+10 hours	10 pm
IDLE - International Date Line NZST - New Zealand	+12 hours	Midnight

Standard NZT - New Zealand		

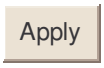
4. **SNTP Sever URL:** Set the SNTP server IP address.
5. **Daylight Saving Period:** Set up the Daylight Saving beginning time and Daylight Saving ending time. Both will be different in every year.
6. **Daylight Saving Offset (mins):** Set up the offset time.
7. **Switch Timer:** Displays the switch current time.
8. Click Apply.



SNTP Configuration interface

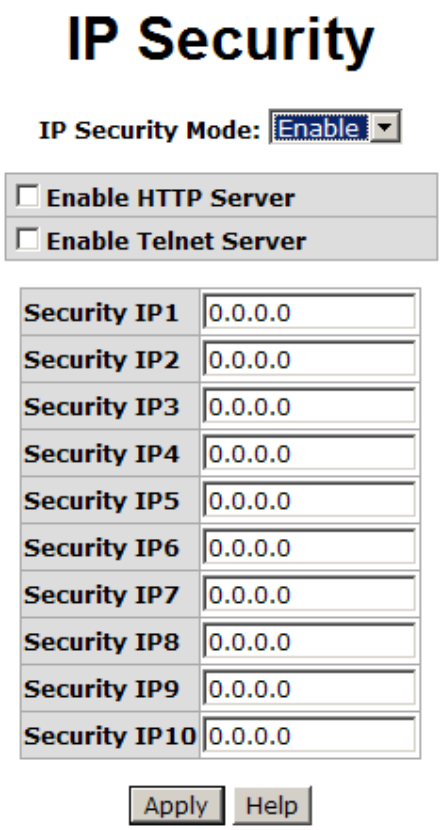
IP Security

The IP security function allows the user to assign 10 specific IP addresses that have permission to access the switch through the web browser for managing the switch.

- **IP Security Mode:** When this option is enabled, the **Enable HTTP Server** and **Enable Telnet Server** Check boxes will then be available.
- **Enable HTTP Server:** When this check box is checked, the IP addresses among Security IP1 ~ IP10 will be allowed to access via HTTP service.
- **Enable Telnet Server:** When checked, the IP addresses among Security IP1 ~ IP10 will be allowed to access via Telnet service.
- **Security IP 1 ~ 10:** Assign up to 10 specific IP addresses. Only these 10 IP address can access and manage the switch through the Web browser
- And then, click 

button to apply the configuration

[NOTE] Remember to execute the “Save Configuration” action, otherwise the new configuration will be lost when switch power is turned off.



IP Security interface

User Authentication

Here you can change login user name and password for management security.

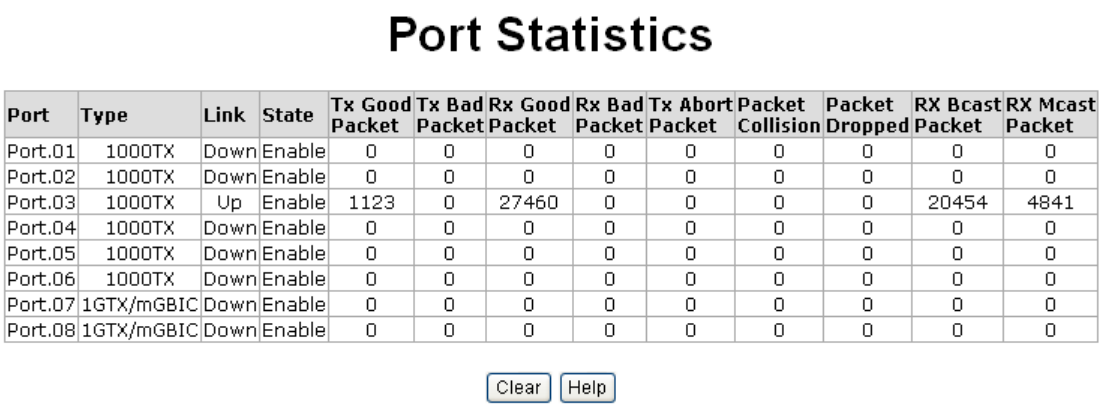
1. **User name:** Key in the new user name (The default is “root”)
2. **Password:** Key in the new password (The default is “root”)
3. **Confirm password:** Re-type the new password
4. And then, click Apply

User Authentication interface

Port Statistics

The following information provides the current port statistic information.

- **Port:** The port number.
- **Type:** Displays the current speed of connection to the port.
- **Link:** The status of linking—'**Up**' or '**Down**'.
- **State:** It's set by Port Control. When the state is disabled, the port will not transmit or receive any packet.
- **Tx Good Packet:** The counts of transmitting good packets via this port.
- **Tx Bad Packet:** The counts of transmitting bad packets (including undersize [less than 64 bytes], oversize, CRC Align errors, fragments and jabbers packets) via this port.
- **Rx Good Packet:** The counts of receiving good packets via this port.
- **Rx Bad Packet:** The counts of receiving bad packets (including undersize [less than 64 bytes], oversize, CRC error, fragments and jabbers) via this port.
- **Tx Abort Packet:** The aborted packet while transmitting.
- **Packet Collision:** The counts of collision packet.
- **Packet Dropped:** The counts of dropped packet.
- **Rx Bcast Packet:** The counts of broadcast packet.
- **Rx Mcast Packet:** The counts of multicast packet.
- Click Clear button to clean all counts.


Port Statistics
Port Type Link State Tx Good Packet Tx Bad Packet Rx Good Packet Rx Bad Packet Tx Abort Packet Packet Collision Packet Dropped RX Bcast Packet RX Mcast Packet
Port.01 1000TX Down Enable 0 0 0 0 0 0 0 0 0
Port.02 1000TX Down Enable 0 0 0 0 0 0 0 0 0
Port.03 1000TX Up Enable 1123 0 27460 0 0 0 0 20454 4841
Port.04 1000TX Down Enable 0 0 0 0 0 0 0 0 0
Port.05 1000TX Down Enable 0 0 0 0 0 0 0 0 0
Port.06 1000TX Down Enable 0 0 0 0 0 0 0 0 0
Port.07 1GTX/mGBIC Down Enable 0 0 0 0 0 0 0 0 0
Port.08 1GTX/mGBIC Down Enable 0 0 0 0 0 0 0 0 0
Clear
Help

Port Statistics interface

Port Control

In Port control, you can view every port status that depended on user setting and the negotiation result.

1. **Port:** select the port that you want to configure.
2. **State:** Current port status. The port can be set to disable or enable mode. If the port setting is disable then will not receive or transmit any packet.
3. **Negotiation:** set auto negotiation status of port.
4. **Speed:** set the port link speed.
5. **Duplex:** set full-duplex or half-duplex mode of the port.
6. **Flow Control:** set flow control function as **Enable** or **Disable** in Full Duplex mode. The default value is **Enable**.
7. **Security:** When its state is '**On**' that means this port accepts only one MAC address which was configured to be a static MAC address.
8. Click Apply.

Port	Group ID	Type	Link	State	Negotiation	Speed Duplex		Flow Control		Security
						Config	Actual	Config	Actual	
Port.01	N/A	1000TX	Down	Enable	Auto	1G Full	N/A	Enable	N/A	OFF
Port.02	N/A	1000TX	Down	Enable	Auto	1G Full	N/A	Enable	N/A	OFF
Port.03	N/A	1000TX	Down	Enable	Auto	1G Full	N/A	Enable	N/A	OFF
Port.04	N/A	1000TX	Down	Enable	Auto	1G Full	N/A	Enable	N/A	OFF
Port.05	N/A	1000TX	Up	Enable	Auto	1G Full	100 Full	Enable	ON	OFF
Port.06	N/A	1000TX	Down	Enable	Auto	1G Full	N/A	Enable	N/A	OFF
Port.07	N/A	1GTX/mGBIC	Down	Enable	Auto	1G Full	N/A	Enable	N/A	OFF
Port.08	N/A	1GTX/mGBIC	Down	Enable	Auto	1G Full	N/A	Enable	N/A	OFF

Port Control interface

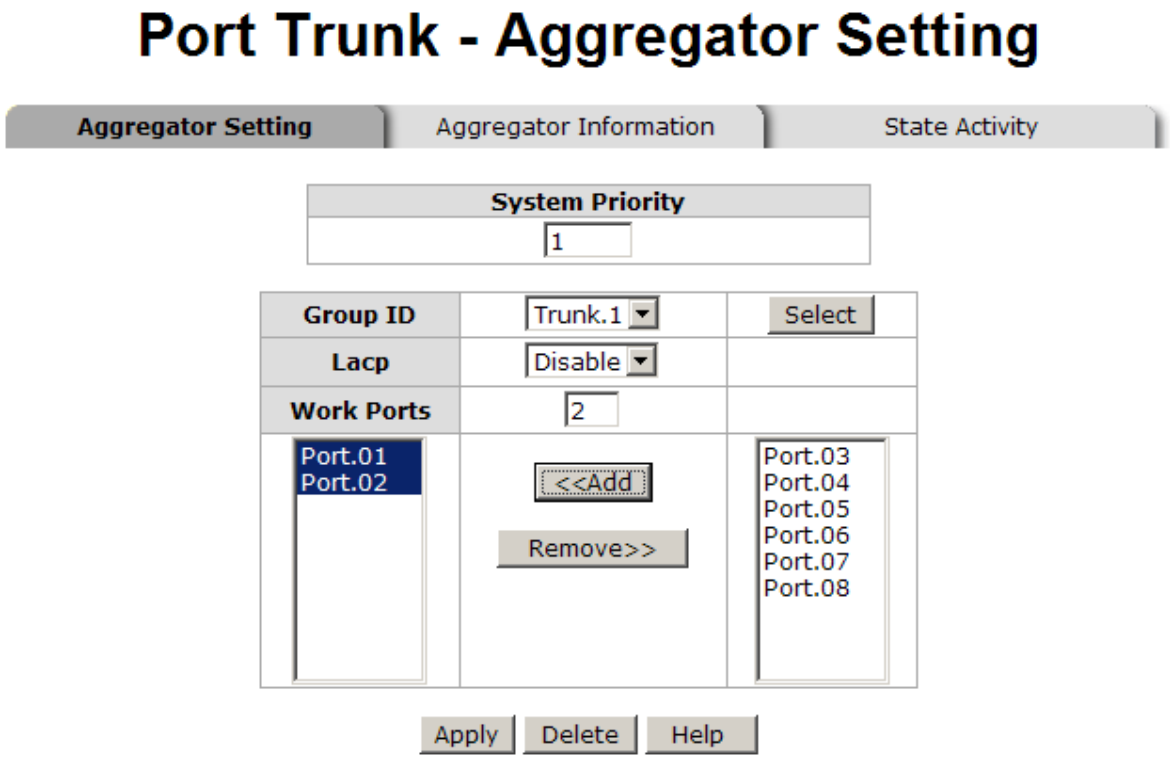
Port Trunk

The Link Aggregation Control Protocol (LACP) provides a standardized means for exchanging information between Partner Systems on a link to allow their Link Aggregation Control instances to reach agreement on the identity of the Link Aggregation Group to which the link belongs, move the link to that Link Aggregation Group, and enable its transmission and reception functions in an orderly manner. Link aggregation lets you group up to 4 ports into one dedicated connection. This feature can expand bandwidth to a device on the network. **LACP operation requires full-duplex mode,** more detail information refers to IEEE 802.3ad.

Aggregator setting

- **System Priority:** A value which is used to identify the active LACP. The switch with the lowest value has the highest priority and is selected as the active LACP.
- **Group ID:** There are four trunk groups to be selected. Choose the "**Group ID**" and click Select.
- **LACP:** When enabled, the trunk group is using LACP. A port which joins an LACP trunk group has to make an agreement with its member ports first. When disabled, the trunk group is a static trunk group. The advantage of having the LACP disabled is that a port joins the trunk group without any handshaking with its member ports. But member ports won't know that they should be aggregated together to form a logic trunk group.
- **Work ports:** This column field allows the user to type in the total number of active port up to four. With LACP static trunk group, e.g. you assign four ports to be the members of a trunk group whose work ports column field is set as two; the exceed ports are standby (the **LACP State Activity** will show 'Passive' on the tab of **State Activity**) and can be aggregated if work ports fail. If it is a static trunk group, the number of work ports must equal the total number of group member ports.
- Select the ports to join the trunk group. The system allows four ports maximum to be aggregated in a trunk group. Click Add to add the port which is focused to the left field. To remove unwanted ports, select the port and click Remove.

- When LACP enabled, you can configure LACP Active/Passive status for each port on State Activity page.
- Click Apply.
- Use Delete to delete Trunk Group. Select the Group ID and click Delete.

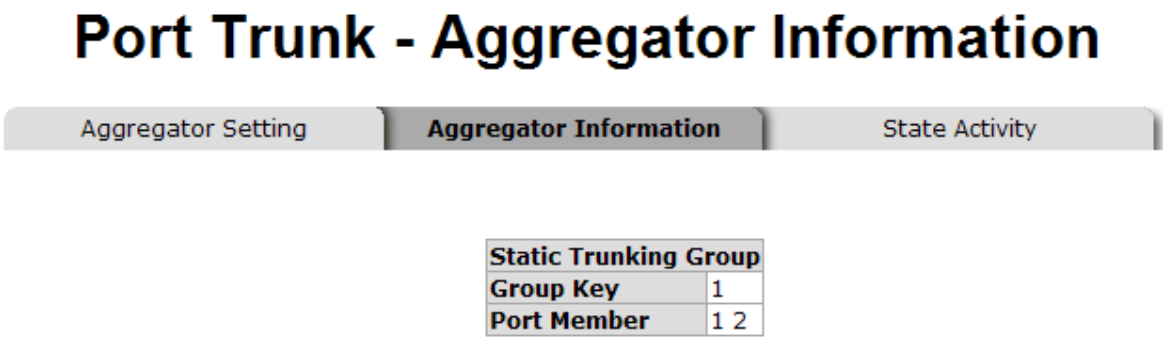


Port Trunk—Aggregator Setting interface

Aggregator Information

When you have setup the aggregator setting with LACP disabled, you will see the local static trunk group information in here.

1. **Group Key:** Displays the trunk group ID.
2. **Port Member:** Displays the members of this static trunk group.



Port Trunk – Aggregator Information interface

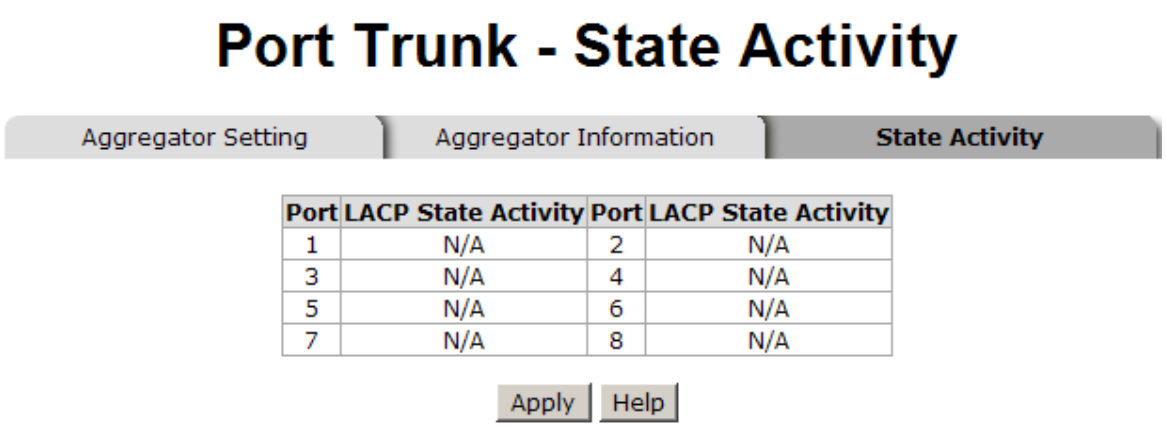
State Activity

Having set up the LACP aggregator on the tab of Aggregator Setting, you can configure the state activity for the members of the LACP trunk group. You can tick or cancel the checkbox beside the state display. When you remove the tick mark to the port and click Apply, the port state activity will change to **Passive**.

- **Active:** The port automatically sends LACP protocol packets.
- **Passive:** The port does not automatically send LACP protocol packets, and responds only if it receives LACP protocol packets from the opposite device.

[NOTE]

1. **A link** having either two active LACP nodes or one active node can perform dynamic LACP trunk.
2. **A link** having two passive LACP nodes will not perform dynamic LACP trunk because both ports are waiting for an LACP protocol packet from the opposite device.

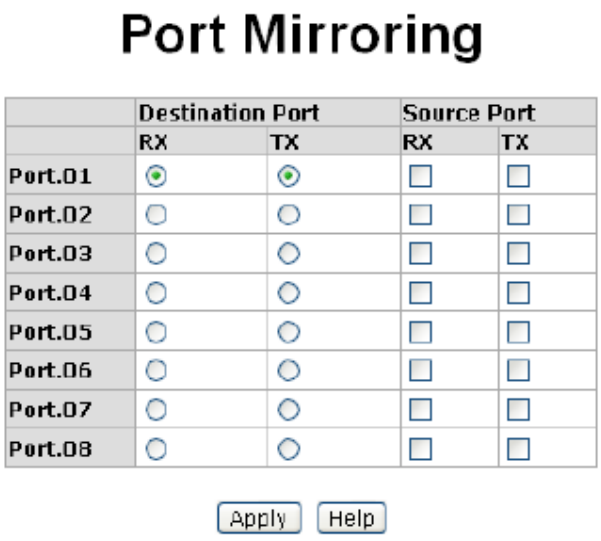


Port Trunk – State Activity interface

Port Mirroring

The Port mirroring is a method for monitoring traffic in switched networks. Traffic through ports can be monitored by one specific port. That means traffic going in or out monitored (source) ports will be duplicated into the mirrored (destination) port.

- **Destination Port:** There is only one port that can be selected to be the destination (mirror) port for monitoring both RX and TX traffic which come from source port. Or, use one of two ports for monitoring RX traffic only and the other one for TX traffic only. User can connect mirror port to LAN analyzer or Netxray
- **Source Port:** The ports that user wants to monitor. All monitored port traffic will be copied to mirror (destination) port. User can select multiple source ports by checking the **RX** or **TX** check boxes to be monitored.
- And then, click Apply button.



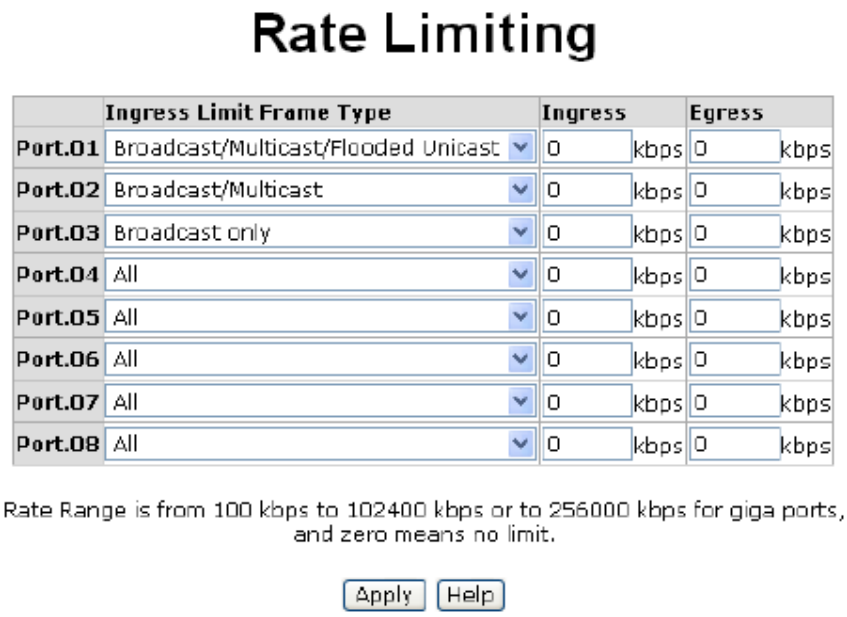
Port Trunk – Port Mirroring interface

Rate Limiting

You can set up every port's bandwidth rate and frame limitation type.

- **Ingress Limit Frame type:** Select the frame type that you want to filter. The frame types have 4 options for selecting: **All, Broadcast/Multicast/Flooded Unicast, Broadcast/Multicast** and **Broadcast only**.

  Broadcast/Multicast/Flooded Unicast, Broadcast/Multicast and **Bbroadcast only** types are only for ingress frames. The egress rate only supports the type of '**All**'.


Rate Limiting
Ingress Limit Frame Type
Ingress
Egress
Port.01 Broadcast/Multicast/Flooded Unicast 0 kbps 0 kbps
Port.02 Broadcast/Multicast 0 kbps 0 kbps
Port.03 Broadcast only 0 kbps 0 kbps
Port.04 All 0 kbps 0 kbps
Port.05 All 0 kbps 0 kbps
Port.06 All 0 kbps 0 kbps
Port.07 All 0 kbps 0 kbps
Port.08 All 0 kbps 0 kbps
Rate Range is from 100 kbps to 102400 kbps or to 256000 kbps for giga ports, and zero means no limit.
Apply
Help

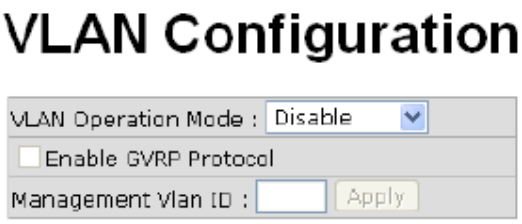
Rate Limiting interface

- All the ports support port ingress and egress rate control. For example, assume port 1 is 10Mbps, users can set its effective egress rate as 1Mbps, ingress rate as 500Kbps. The switch performs the ingress rate by packet counter to meet the specified rate
  - **Ingress:** Enter the port effective ingress rate (The default value is "0")
  - **Egress:** Enter the port effective egress rate (The default value is "0")
- And then, click Apply to apply the settings.

VLAN configuration

A Virtual LAN (VLAN) is a logical network grouping that limits the broadcast domain. This enables isolation of network traffic, so only the members of the VLAN will receive traffic from the same VLAN members. Basically, creating a VLAN from a switch is logically equivalent to reconnecting a group of network devices to another Layer 2 switch. However, all the network devices are still plugged into the same switch physically.

The industrial switch supports port-based and 802.1Q (tagged-based) VLAN. The default configuration of VLAN operation mode is "**Disable**".



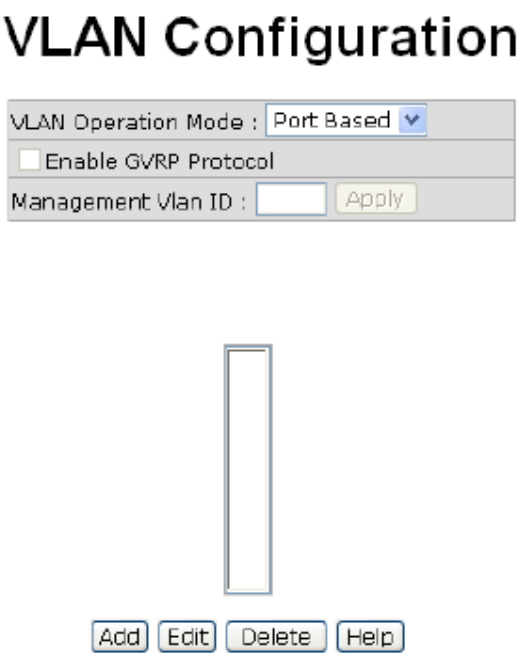
VLAN NOT ENABLE

VLAN Configuration interface

VLAN configuration—Port-based VLAN

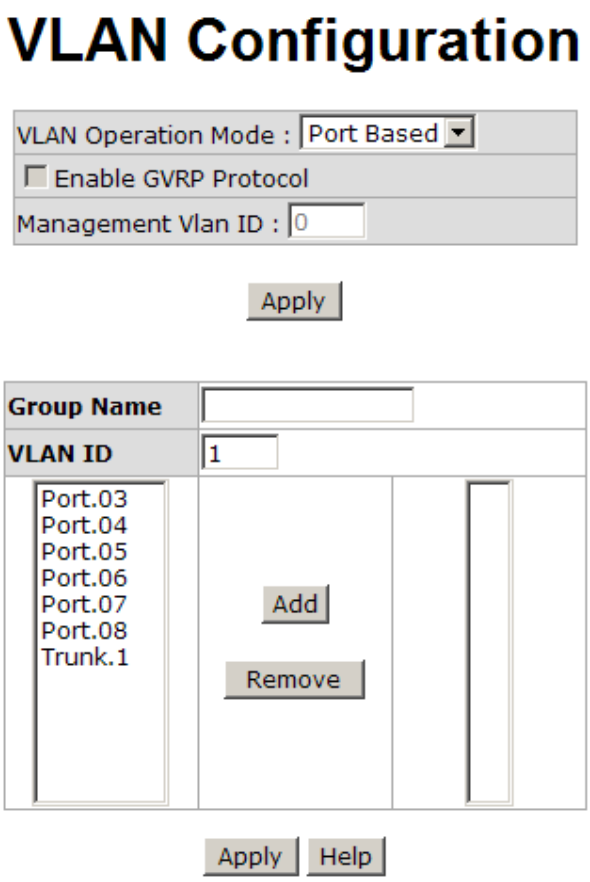
Packets can go among only members of the same VLAN group. Note all unselected ports are treated as belonging to another single VLAN. If port-based VLAN is enabled, the VLAN-tagging is ignored.

In order for an end station to send packets to different VLAN groups, it itself has to be either capable of tagging packets it sends with VLAN tags, or it must be attached to a VLAN-aware bridge that is capable of classifying and tagging the packet with a different VLAN ID based on not only default PVID but also other information about the packet, such as the protocol.



VLAN – Port Based interface

- Click Add to add a new VLAN group(The maximum VLAN group is up to 256 VLAN groups)
- Entering the VLAN name, group ID and grouping the members of VLAN group
- And then, click Apply



VLAN—Port Based Add interface

- You will see the VLAN displays.
- Use Delete button to delete unwanted VLAN.
- Use Edit button to modify existing VLAN group.

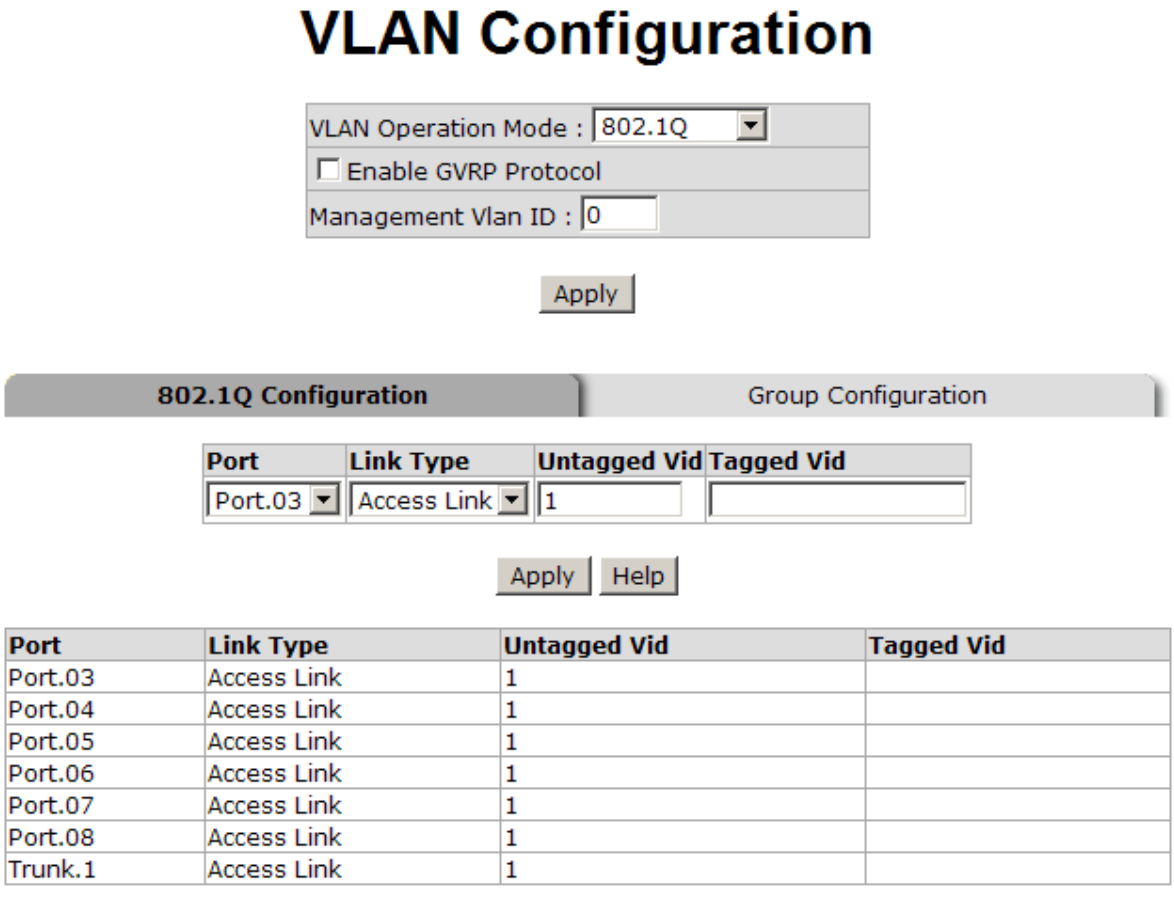
Note	Remember to execute the 'Save Configuration' action, otherwise the new configuration will be lost when switch power is removed.

802.1Q VLAN

Tag-based VLAN is an IEEE 802.1Q specification standard. Therefore, it is possible to create a VLAN across devices from different switch venders. IEEE 802.1Q VLAN uses a technique to insert a “tag” into the Ethernet frames. The Tag contains a VLAN Identifier (VID) that indicates the VLAN numbers.

You can create a Tag-based VLAN, and enable or disable GVRP protocol. There are 256 VLAN groups. If 802.1Q VLAN is Enabled then all ports on the switch belong to the default VLAN, VID is 1. The default VLAN can’t be deleted.

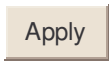
GVRP allows automatic VLAN configuration between the switch and nodes. If the switch is connected to a device with GVRP enabled, you can send a GVRP request using the VID of a VLAN defined on the switch; the switch will automatically add that device to the existing VLAN.



Port	Link Type	Untagged Vid	Tagged Vid
Port.03	Access Link	1	
Port.04	Access Link	1	
Port.05	Access Link	1	
Port.06	Access Link	1	
Port.07	Access Link	1	
Port.08	Access Link	1	
Trunk.1	Access Link	1	

802.1q VLAN interface

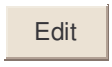
802.1Q Configuration

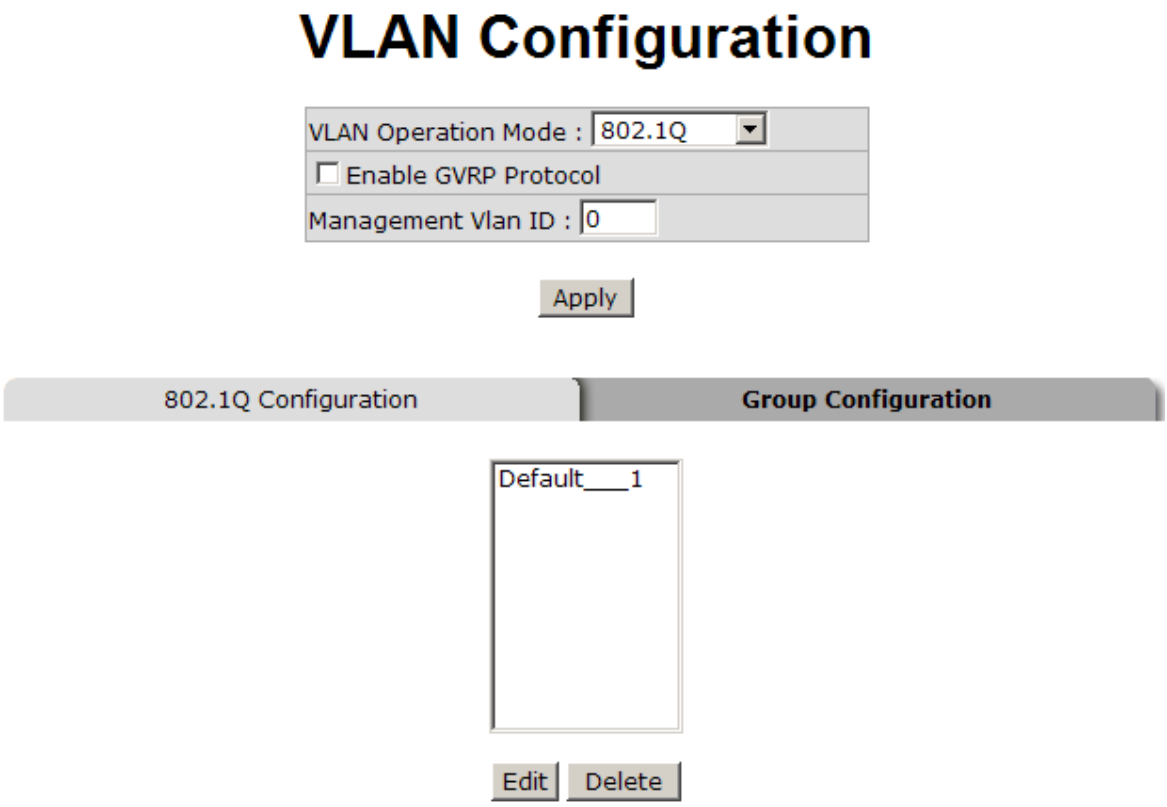
1. **Enable GVRP Protocol:** check the check box to enable GVRP protocol.
2. Select the port that you want to configure.
3. **Link Type**: There are 3 types of link type.
   - **Access Link:** Single switch only, allows user to group ports by setting the same VID to those ports.
   - **Trunk Link:** The extended application of **Access Link**. While the ports are set in this type, they can forward the packets with specified tag among the switches which are included in the same VLAN group.
   - **Hybrid Link:** Both **Access Link** and **Trunk Link** are available.
4. **Untagged VID:** assign the untagged frame VID.
5. **Tagged VID:** assign the tagged frame VID.
6. Click 

7. You can see each port setting in the below table on the screen.

Group Configuration

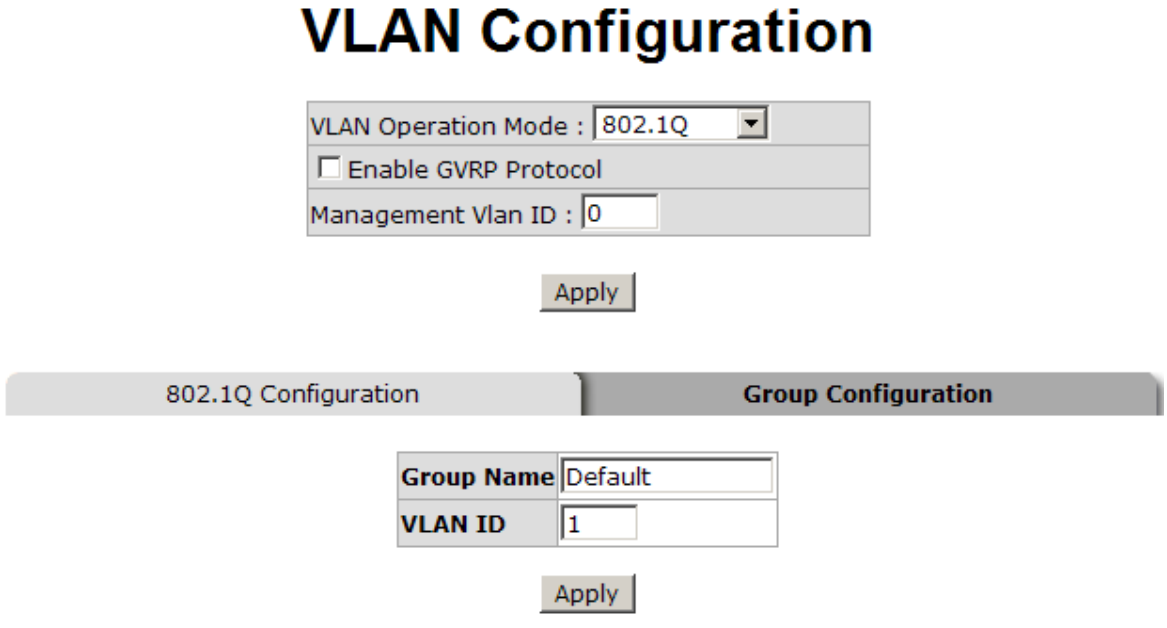
Edit the existing VLAN Group.

1. Select the VLAN group in the table list.
2. Click 



Group Configuration interface

3. You can Change the VLAN group name and VLAN ID.
4. Click Apply.



Group Configuration interface

Rapid Spanning Tree

The Rapid Spanning Tree Protocol (RSTP) is an evolution of the Spanning Tree Protocol and provides for faster spanning tree convergence after a topology change. The system also supports STP and the system will auto detect the connected device that is running STP or RSTP protocol.

RSTP - System Configuration

- User can view spanning tree information about the Root Bridge.
- User can modify RSTP state. After modification, click Apply button
  - **RSTP mode:** User must enable or disable RSTP function before configure the related parameters.
  - **Priority (0-61440):** A value used to identify the root bridge. The bridge with the lowest value has the highest priority and is selected as the root. The value must be a multiple of 4096 according to the protocol standard rule.
  - **Max Age (6-40):** The number of seconds a bridge waits without receiving Spanning-tree Protocol configuration messages before attempting a reconfiguration. Enter a value between 6 through 40.
  - **Hello Time (1-10):** The time that controls switch sends out the BPDU packet to check RSTP current status. Enter a value between 1 through 10.
  - **Forward Delay Time (4-30):** The number of seconds a port waits before changing from its Rapid Spanning-Tree Protocol learning and listening to STP states to the forwarding state. Enter a value between 4 through 30.

Note	Follow the rule to configure the MAX Age, Hello Time, and Forward Delay Time. **2 x (Forward Delay Time value – 1) > = Max Age value >= 2 x (Hello Time value +1)**

RSTP - System Configuration

System Configuration | Port Configuration

RSTP Mode	Enable
Priority (0-61440)	32768
Max Age (6-40)	20
Hello Time (1-10)	2
Forward Delay Time (4-30)	15

Priority must be a multiple of 4096
2*(Forward Delay Time-1) should be greater than or equal to the Max Age.
The Max Age should be greater than or equal to 2*(Hello Time + 1).

Apply Help

Root Bridge Information

Bridge ID	0080000F380131DD
Root Priority	32768
Root Port	Root
Root Path Cost	0
Max Age	20
Hello Time	2
Forward Delay	15

RSTP System Configuration interface

RSTP - Port Configuration

You can configure path cost and priority of every port.

1. **Path Cost:** The cost of the path to the other bridge from this transmitting bridge at the specified port. Enter a number 1 through 200000000.
2. **Priority:** Decide which port should be blocked by priority in LAN. Enter a number 0 through 240. The value of priority must be the multiple of 16.
3. **P2P:** Some of the rapid state transactions that are possible within RSTP are dependent upon whether the port concerned can only be connected to exactly one other bridge (i.e. it is served by a point-to-point LAN segment), or can be connected to two or more bridges (i.e. it is served by a shared medium LAN segment). This function allows the P2P status of the link to be manipulated administratively. True is P2P enabling. False is P2P disabling.
4. **Edge:** The port directly connected to end stations cannot create bridging loop in the network. To configure the port as an edge port, set the port to "**True**" status.
5. **Non Stp:** The port includes the STP mathematic calculation. **True** is not including STP mathematic calculation. **False** is including the STP mathematic calculation.
6. Click Apply.

RSTP - Port Configuration

System Configuration | **Port Configuration**

Port	Path Cost (1-200000000)	Priority (0-240)	Admin P2P	Admin Edge	Admin Non Stp
Port.01 Port.02 Port.03 Port.04 Port.05	20000(	128	Auto	true	false

priority must be a multiple of 16

Apply Help

RSTP Port Status

Port	Path Cost	Port Priority	Oper P2P	Oper Edge	Stp Neighbor	State	Role
Port.01	20000	128	True	True	False	Disabled	Disabled
Port.02	20000	128	True	True	False	Disabled	Disabled
Port.03	20000	128	True	True	False	Disabled	Disabled
Port.04	20000	128	True	True	False	Disabled	Disabled
Port.05	20000	128	True	True	False	Forwarding	Designated
Port.06	20000	128	True	True	False	Disabled	Disabled
Port.07	20000	128	True	True	False	Disabled	Disabled
Port.08	20000	128	True	True	False	Disabled	Disabled

RSTP Port Configuration interface

SNMP Configuration

Simple Network Management Protocol (SNMP) is the protocol developed to manage nodes (servers, workstations, routers, switches and hubs etc.) on an IP network. SNMP enables network administrators to manage network performance, find and solve network problems, and plan for network growth. Network management systems learn of problems by receiving traps or change notices from network devices implementing SNMP.

System Configuration

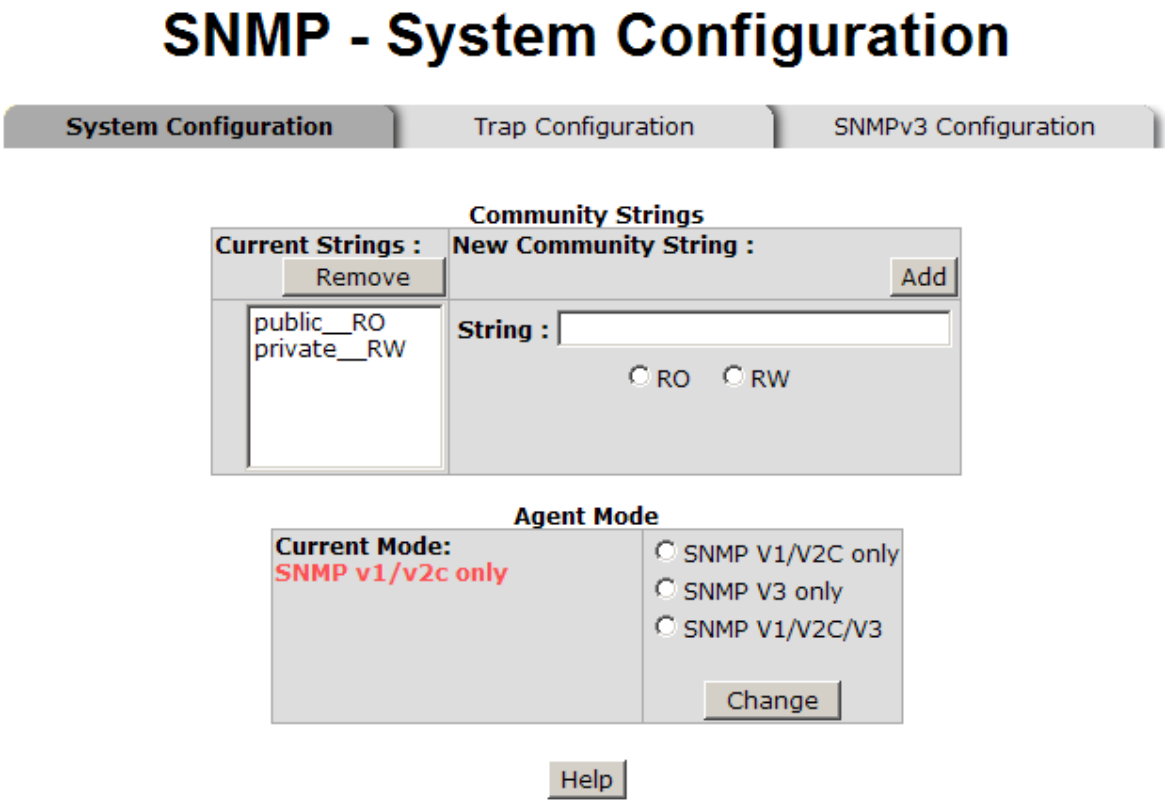
- **Community Strings**

You can define a new community string set or remove unwanted community string.

1. **String:** Fill the name of string.
2. **RO:** Read only. Enables requests accompanied by this string to display MIB-object information.
3. **RW:** Read write. Enables requests accompanied by this string to display MIB-object information and to set MIB objects.

1. Click Add.
2. To remove the community string, select the community string that you have defined and click Remove. You cannot edit the name of the default community string set.

- **Agent Mode:** Select the SNMP version that you want to use it. And then click Change to switch to the selected SNMP version mode.

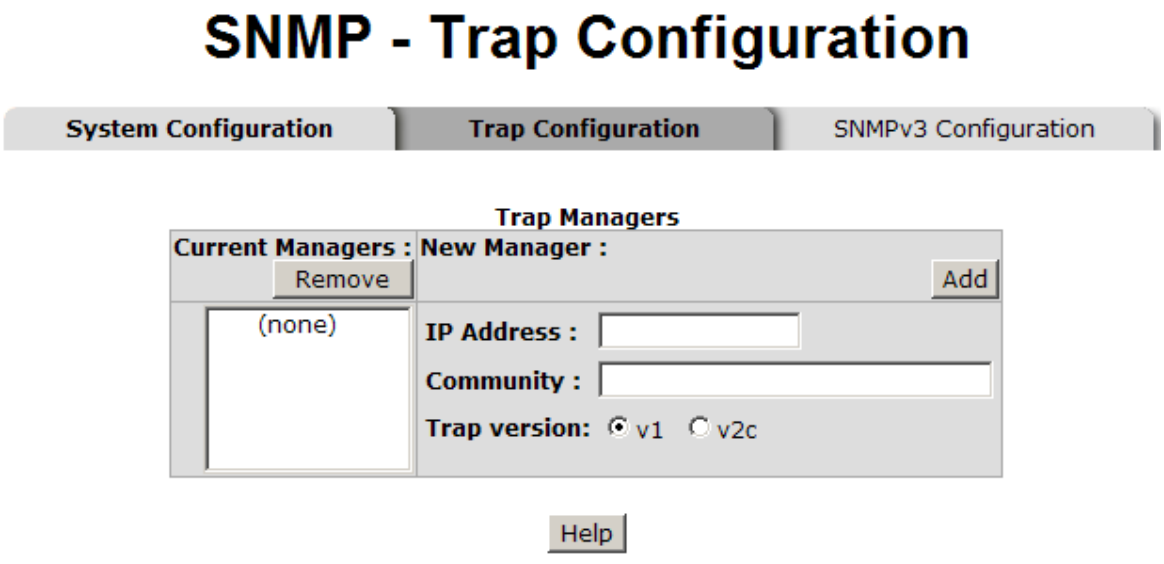


SNMP System Configuration interface

Trap Configuration

A trap manager is a management station that receives traps, the system alerts generated by the switch. If no trap manager is defined, no traps will issue. Create a trap manager by entering the IP address of the station and a community string. To define management stations as trap manager and enter SNMP community strings and selects the SNMP version.

1. **IP Address:** Enter the IP address of trap manager.
2. **Community:** Enter the community string.
3. **Trap Version:** Select the SNMP trap version type—v1 or v2c.
4. Click Add.
5. To remove the community string, select the community string that you have defined and click Remove. You cannot edit the name of the default community string set.



Trap Managers interface

SNMPV3 Configuration

Configure the SNMP V3 function.

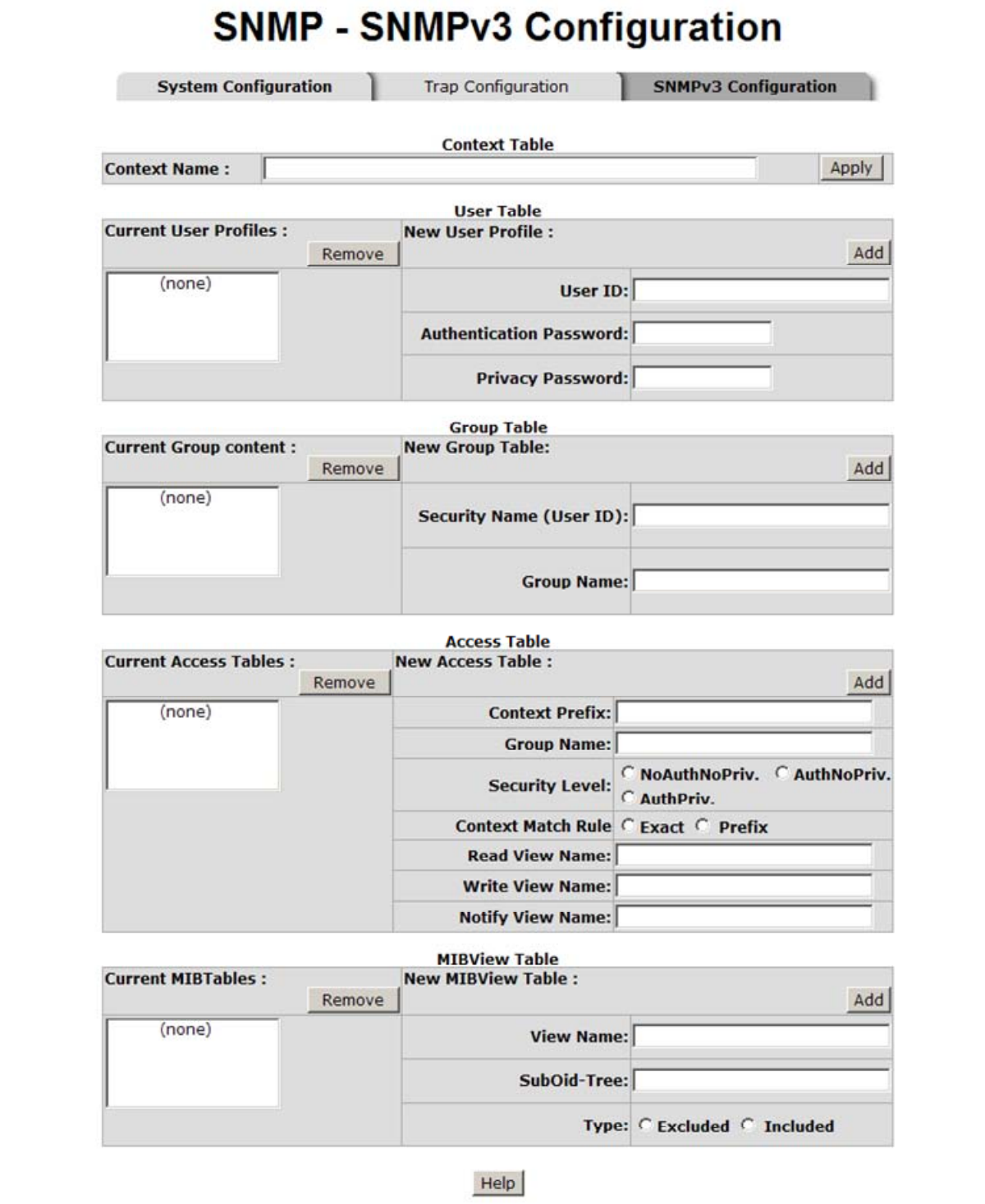
Context Table

Configure SNMP v3 context table. Assign the context name of context table. Click Add to add context name. Click Remove to remove unwanted context name.

User Profile

Configure SNMP v3 user table..

- **User ID:** Set up the user name.
- **Authentication Password:** Set up the authentication password.
- **Privacy Password:** Set up the private password.
- Click Add to add context name.
- Click Remove to remove unwanted context name.



SNMP V3 configuration interface

Group Table

Configure SNMP v3 group table.

- **Security Name (User ID):** Assign the user name that you have set up in user table.
- **Group Name:** Set up the group name.
- Click Add to add context name.
- Click Remove to remove unwanted context name.

Access Table

Configure SNMP v3 access table.

- **Context Prefix:** Set up the context name.
- **Group Name:** Set up the group.
- **Security Level:** Select the access level.
- **Context Match Rule:** Select the context match rule.
- **Read View Name:** Set up the read view.
- **Write View Name:** Set up the write view.
- **Notify View Name:** Set up the notify view.
- Click Add to add context name.
- Click Remove to remove unwanted context name.

MIBview Table

Configure MIB view table.

- **ViewName:** Set up the name.
- **Sub-Oid Tree:** Fill the Sub-OID.
- **Type:** Select the type – exclude or included.
- Click Add to add context name.
- Click Remove to remove unwanted context name.

QoS Configuration

You can configure Qos policy and priority setting, per port priority setting, COS and TOS setting.

QoS Policy and Priority Type

- **Qos Policy:** select the Qos policy rule.
  - **Using the 8,4,2,1 weight fair queue scheme:** The switch will follow 8:4:2:1 rate to process priority queue from High to lowest queue. For example, when the system processes, 1 frame of the lowest queue, 2 frames of the low queue, 4 frames of the middle queue, and 8 frames of the high queue will be processed at the same time in accordance with the 8,4,2,1 policy rule.
  - **Use the strict priority scheme:** Always higher queue will be process first, except higher queue is empty.
- **Priority Type:** there are 5 priority type selections available. Disable means no priority type is selected.
- **Port-base:** the port priority will follow the **Port-base** that you have assigned – High, middle, low, or lowest.
  - **COS only:** the port priority will only follow the **COS priority** that you have assigned.
  - **TOS only:** the port priority will only follow the **TOS priority** that you have assigned.
  - **COS first:** the port priority will follow the COS priority first, and then other priority rule.
  - **TOS first:** the port priority will follow the TOS priority first, and the other priority rule.
- Click Apply.

QoS Configuration

Qos Policy:

Use an 8,4,2,1 weighted fair queuing scheme
Use a strict priority scheme
Priority Type: Disable

Apply Help

Port-based Priority:

Port.01	Port.02	Port.03	Port.04	Port.05	Port.06	Port.07	Port.08
Lowest	Lowest	Lowest	Lowest	Lowest	Lowest	Lowest	Lowest

Apply Help

COS:

Priority	0	1	2	3	4	5	6	7
	Lowest	Lowest	Lowest	Lowest	Lowest	Lowest	Lowest	Lowest

Apply Help

TOS:

Priority	0	1	2	3	4	5	6	7
	Lowest	Lowest	Lowest	Lowest	Lowest	Lowest	Lowest	Lowest
Priority	8	9	10	11	12	13	14	15
	Lowest	Lowest	Lowest	Lowest	Lowest	Lowest	Lowest	Lowest
Priority	16	17	18	19	20	21	22	23
	Lowest	Lowest	Lowest	Lowest	Lowest	Lowest	Lowest	Lowest
Priority	24	25	26	27	28	29	30	31
	Lowest	Lowest	Lowest	Lowest	Lowest	Lowest	Lowest	Lowest
Priority	32	33	34	35	36	37	38	39
	Lowest	Lowest	Lowest	Lowest	Lowest	Lowest	Lowest	Lowest
Priority	40	41	42	43	44	45	46	47
	Lowest	Lowest	Lowest	Lowest	Lowest	Lowest	Lowest	Lowest
Priority	48	49	50	51	52	53	54	55
	Lowest	Lowest	Lowest	Lowest	Lowest	Lowest	Lowest	Lowest
Priority	56	57	58	59	60	61	62	63
	Lowest	Lowest	Lowest	Lowest	Lowest	Lowest	Lowest	Lowest

Apply Help

QoS Configuration interface

Port Base Priority

Configure per port priority level.

- **Port:** Each port has 4 egress queues – High, Middle, Low, and Lowest.
- Click Apply.

COS Configuration

Set up the COS priority level.

- **COS priority:** Set up the COS priority level 0~7 with 4 egress queues: High, Middle, Low, Lowest.
- Click Apply.

TOS Configuration

Set up the TOS priority.

- **TOS priority:** the system provides 0~63 TOS priority level. Each level has 4 types of priority (egress queues) – high, middle, low, and lowest. The default value is “Lowest” priority for each level. When the IP packet is received, the system will check the TOS level value in the IP packet that has received. For example, user set the TOS level 25 as high, the system will check the TOS value of the received IP packet. If the TOS value of received IP packet is 25(priority = high), and then the packet priority will have highest priority.
- Click Apply.

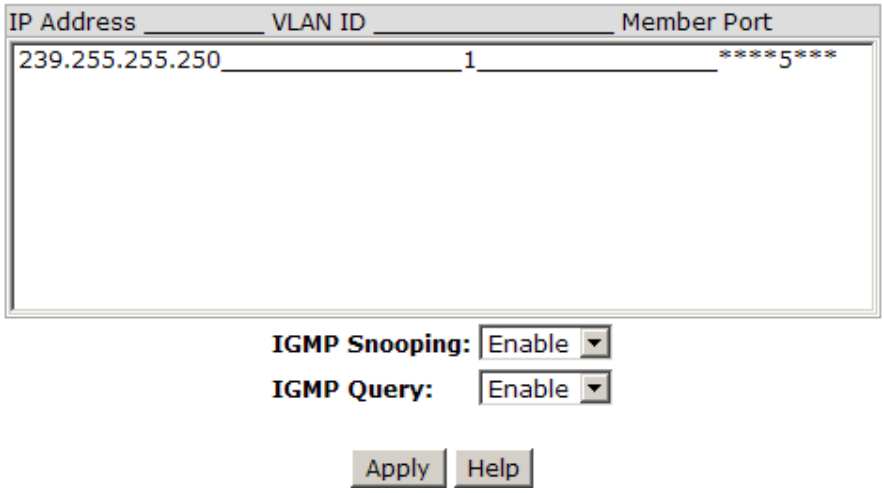
IGMP Configuration

The Internet Group Management Protocol (IGMP) is an internal protocol of the Internet Protocol (IP) suite. IP manages multicast traffic by using switches, routers, and hosts that support IGMP. Enabling IGMP allows the ports to detect IGMP queries and report packets and manage IP multicast traffic through the switch. IGMP has three fundamental types of message as follows:

Message	Description
Query	A message sent from the querier (IGMP router or switch) asking for a response from each host belonging to the multicast group.
Report	A message sent by a host to the querier to indicate that the host wants to be or is a member of a given group indicated in the report message.
Leave Group	A message sent by a host to the querier to indicate that the host has quit being a member of a specific multicast group.

The switch supports IP multicast. You can enable IGMP protocol via setting IGMP configuration page to see the IGMP snooping information. IP multicast addresses are in the range of 224.0.0.0 through 239.255.255.255.

- **IGMP Protocol:** Enable or disable the IGMP protocol.
- **IGMP Query:** Select the IGMP query function as Enable or Auto to set the switch as a querier for IGMP version 2 multicast network.
- Click Apply.



IGMP Configuration interface

X-Ring

X-Ring provides a faster redundant recovery than Spanning Tree topology. The action is similar to STP or RSTP, but the algorithms are different.

In the X-Ring topology, every switch should enable X-Ring function and assign two member ports for connecting to the ring. Only one switch in the X-Ring group would be set as the master switch with one of the member ports blocked, called backup port, and another port is called working port. Other switches in the X-Ring group are called working switches and their two member ports are called working ports. When a failure of a network connection occurs, the backup port will automatically become a working port to recover from the failure.

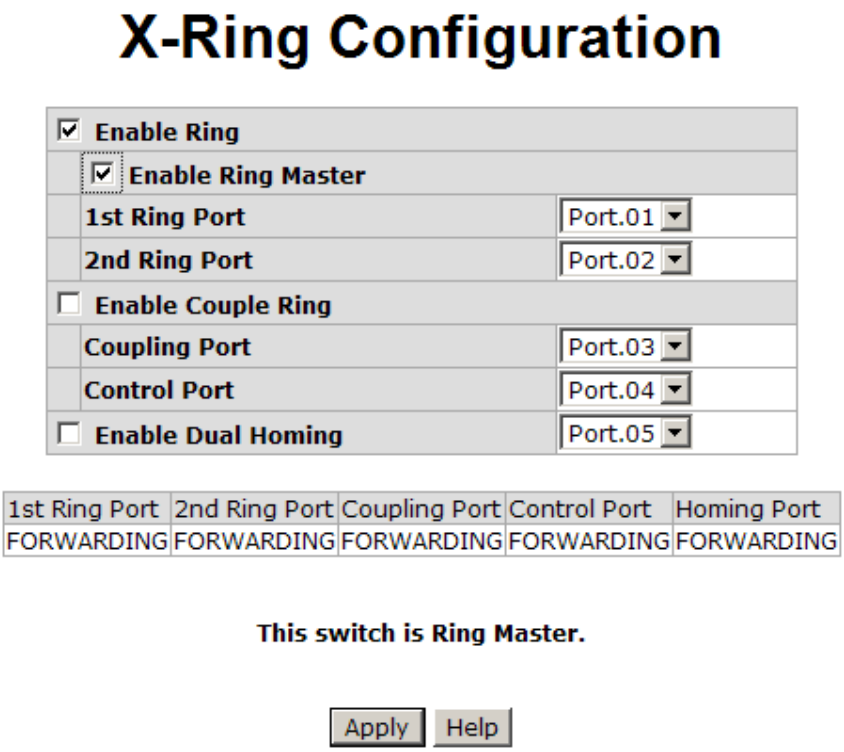
The switch supports the function and interface for setting the switch as the ring master or slave mode. The ring master can negotiate and command other switches in the X-Ring group. If there are 2 or more switches in master mode, then software will select the switch with lowest MAC address number as the ring master. The X-Ring master ring mode will be enabled by the X-Ring configuration interface. Also, users can identify the switch as the ring master when the R.M. LED on the switch is lit.

The system also supports the coupling ring that can connect 2 or more X-Ring group for the redundant backup function and dual homing function that prevents lost connection between an X-Ring group and an upper level/core switch.

- **Enable X-Ring:** To enable the X-Ring function. Marking the check box to enable the X-Ring function.
- **Enable Ring Master:** Mark the check box for enabling this machine to be a ring master.
- **1st & 2nd Ring Ports:** Pull down the selection menu to assign two ports as the member ports. The **1st Ring Port** and **2nd Ring Port** are basically assigned to be forwarding ports except for the Ring Master switch. With the Ring Master switch, one of its two Ring Ports is the blocking port and another one is the forwarding port. Once its forwarding port fails, the system will automatically upgrade its blocking port

to be the forwarding port of the Ring Master switch.

- **Enable Coupling Ring:** To enable the coupling ring function. Marking the check box to enable the coupling ring function.
- **Coupling port:** Assign the member port which is connected to the other ring group.
- **Control port:** When Couple Ring check box is marked, you have to assign the control port to form a couple-ring group between the two X-rings.
- **Enable Dual Homing:** Set up one of the ports on the switch to be the Dual Homing port. For a switch, there is only one Dual Homing port. Dual Homing only works while the X-Ring function enabled.
- And then, click Apply to apply the configuration.



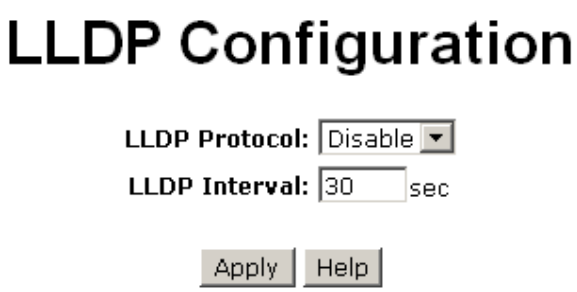
X-ring Interface

Note	When the X-Ring function enable, user must disable the RSTP. The X-Ring function and RSTP function cannot exist in a switch at the same time. Remember to execute the 'Save Configuration' action, otherwise the new configuration will be lost when switch power is removed.

LLDP Configuration

Link Layer Discovery Protocol (LLDP) is defined in the IEEE 802.1AB. It is an emerging standard which provides a solution for the configuration issues caused by expanding LANs. LLDP specifically defines a standard method for Ethernet network devices such as switches, routers and wireless LAN access points to advertise information about themselves to other nodes on the network and store the information they discover. LLDP runs on all 802 media. The protocol runs over the data-link layer only, allowing two systems running different network layer protocols to learn about each other.

- **LLDP Protocol**: Pull down the selection menu to disable or enable LLDP function.
- **LLDP Interval**: Set the interval of advertising the switch's information to other nodes.
- Click Apply.



LLDP Interface

Security

In this section, you can configure 802.1x and MAC address table.

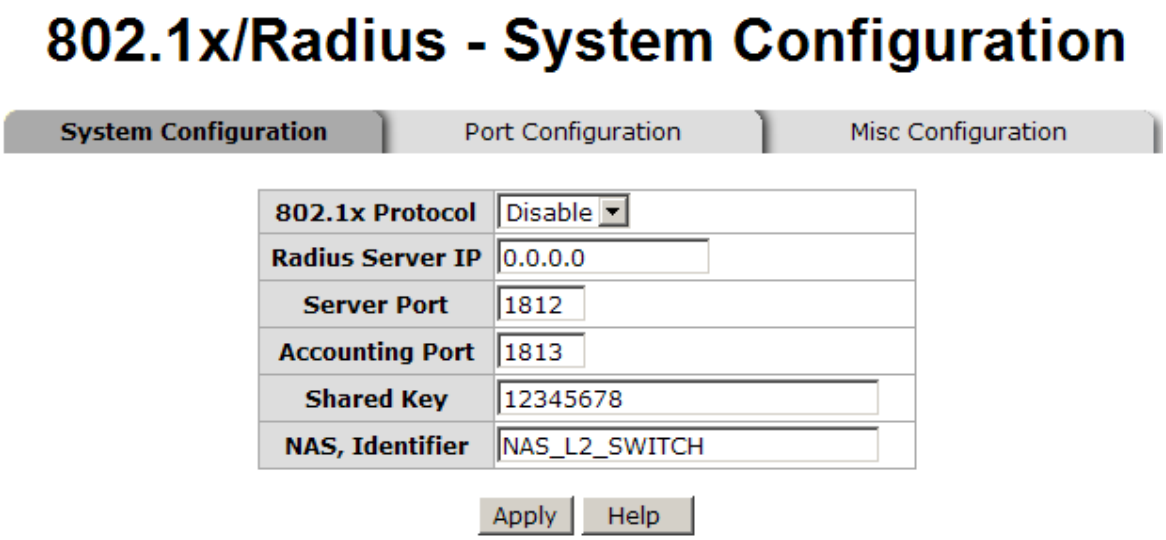
802.1X/Radius Configuration

802.1x is an IEEE authentication specification that prevents the client from accessing the wireless access point or wired switch until it provides authority, like the user name/password that are verified by an authentication server.

System Configuration

After enabling the IEEE 802.1X function, you can configure the parameters of this function.

1. **IEEE 802.1x Protocol:** Enable or disable 802.1x protocol.
2. **Radius Server IP:** Set the Radius Server IP address.
3. **Server Port:** Set the UDP destination port for authentication requests to the specified Radius Server.
4. **Accounting Port:** Set the UDP destination port for accounting requests to the specified Radius Server.
5. **Shared Key:** Set an encryption key for using during authentication sessions with the specified radius server. This key must match the encryption key used on the Radius Server.
6. **NAS, Identifier:** Set the identifier for the radius client.
7. Click Apply.

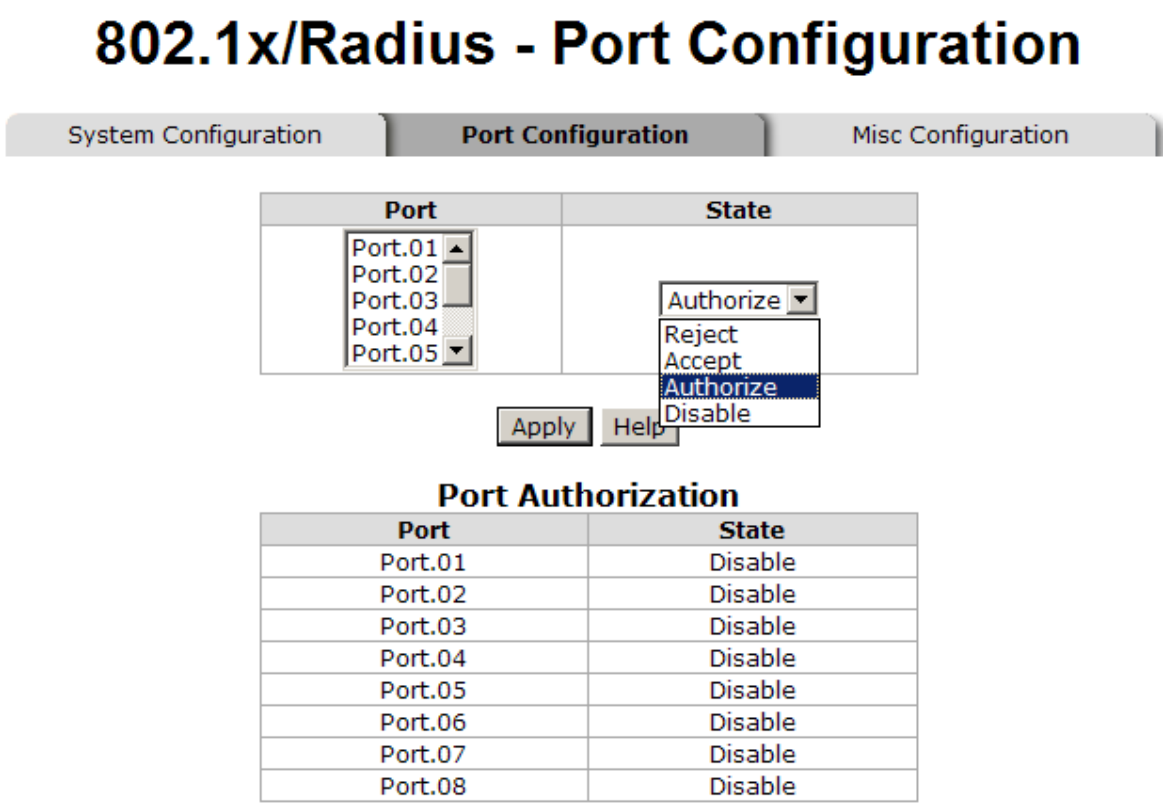


802.1x System Configuration interface

802.1x Port Configuration

You can configure 802.1x authentication state for each port. The State provides Disable, Accept, Reject and Authorize.

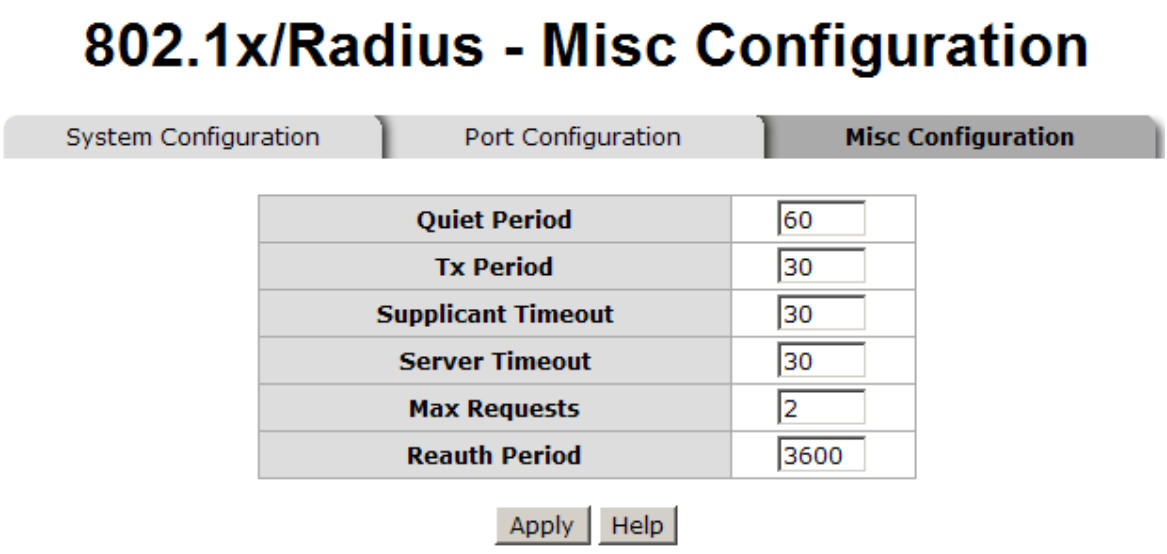
- **Reject:** The specified port is required to be held in the unauthorized state.
- **Accept:** The specified port is required to be held in the Authorized state.
- **Authorized:** The specified port is set to the Authorized or Unauthorized state in accordance with the outcome of an authentication exchange between the Supplicant and the authentication server.
- **Disable:** When disabled, the specified port works without complying with 802.1x protocol.
- Click Apply.



802.1x Per Port Setting interface

Misc Configuration

1. **Quiet Period:** Set the period during which the port doesn't try to acquire a supplicant.
2. **TX Period:** Set the period the port wait for retransmit next EAPOL PDU during an authentication session.
3. **Supplicant Timeout:** Set the period of time the switch waits for a supplicant response to an EAP request.
4. **Server Timeout:** Set the period of time the switch waits for a server response to an authentication request.
5. **Max Requests:** Set the number of authentication that must time-out before authentication fails and the authentication session ends.
6. **Reauth period:** Set the period of time after which clients connected must be re-authenticated.
7. Click Apply.



802.1x Misc Configuration interface

MAC Address Table

Use the MAC address table to ensure port security.

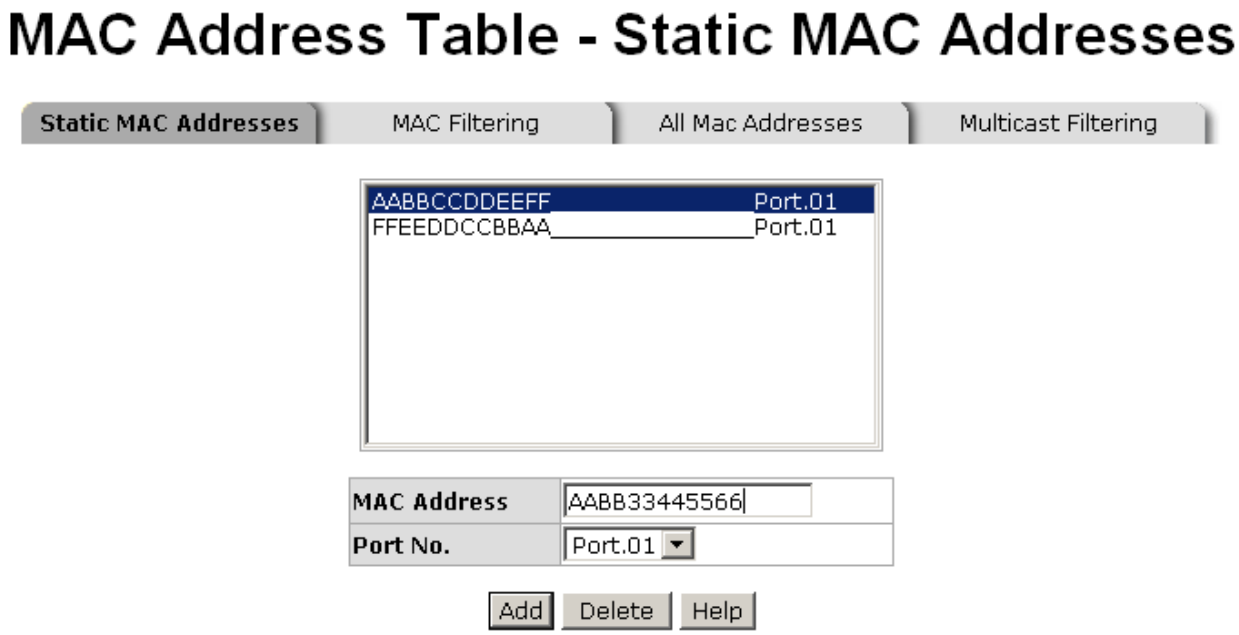
Static MAC Address

You can add a static MAC address; it remains in the switch's address table, regardless of whether the device is physically connected to the switch. This saves the switch from having to re-learn a device's MAC address when the disconnected or powered-off device is active on the network again. You can add / modify / delete a static MAC address.

Add the Static MAC Address

You can add static MAC address in the switch MAC table here.

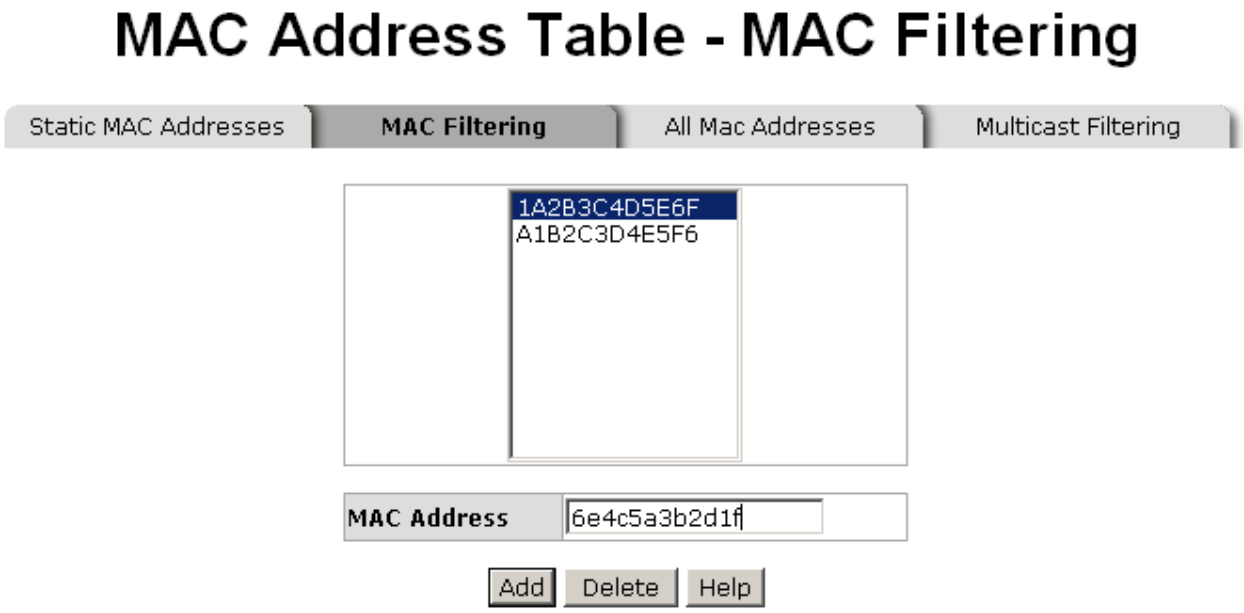
- **MAC Address:** Enter the MAC address of the port that should permanently forward traffic, regardless of the device network activity.
- **Port No.:** Pull down the selection menu to select the port number.
- Click Add.
- If you want to delete the MAC address from filtering table, select the MAC address and click Delete.



Static MAC Addresses interface

MAC Filtering

By filtering MAC addresses, the switch can easily filter the pre-configured MAC address and reduce insecurity. You can add and delete filtering MAC address.



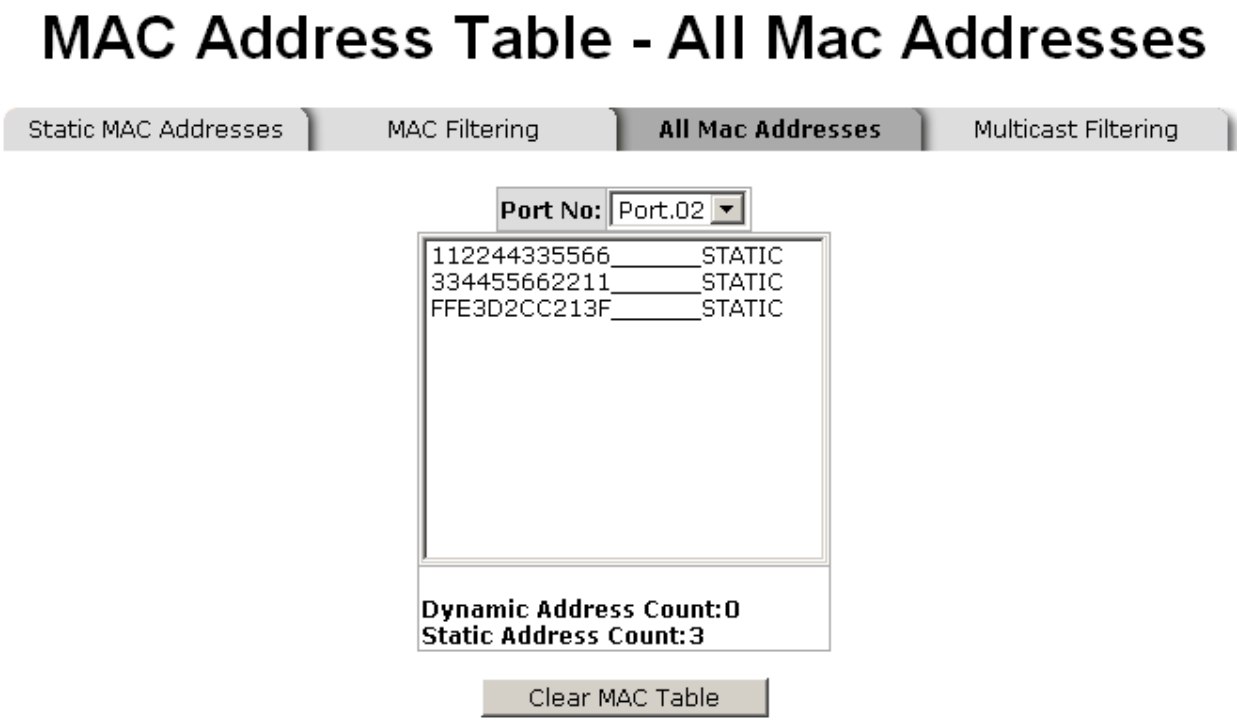
MAC Filtering interface

- **MAC Address:** Enter the MAC address that you want to filter.
- Click Add.
- If you want to delete the MAC address from the filtering table, select the MAC address and click Delete.

All MAC Addresses

You can view all of the MAC addresses learned by the selected port.

- Select the port number.
- The selected port of static & dynamic MAC address information will be displayed in here.
- Click Clear MAC Table to clear the dynamic MAC addresses information of the current port shown on the screen.

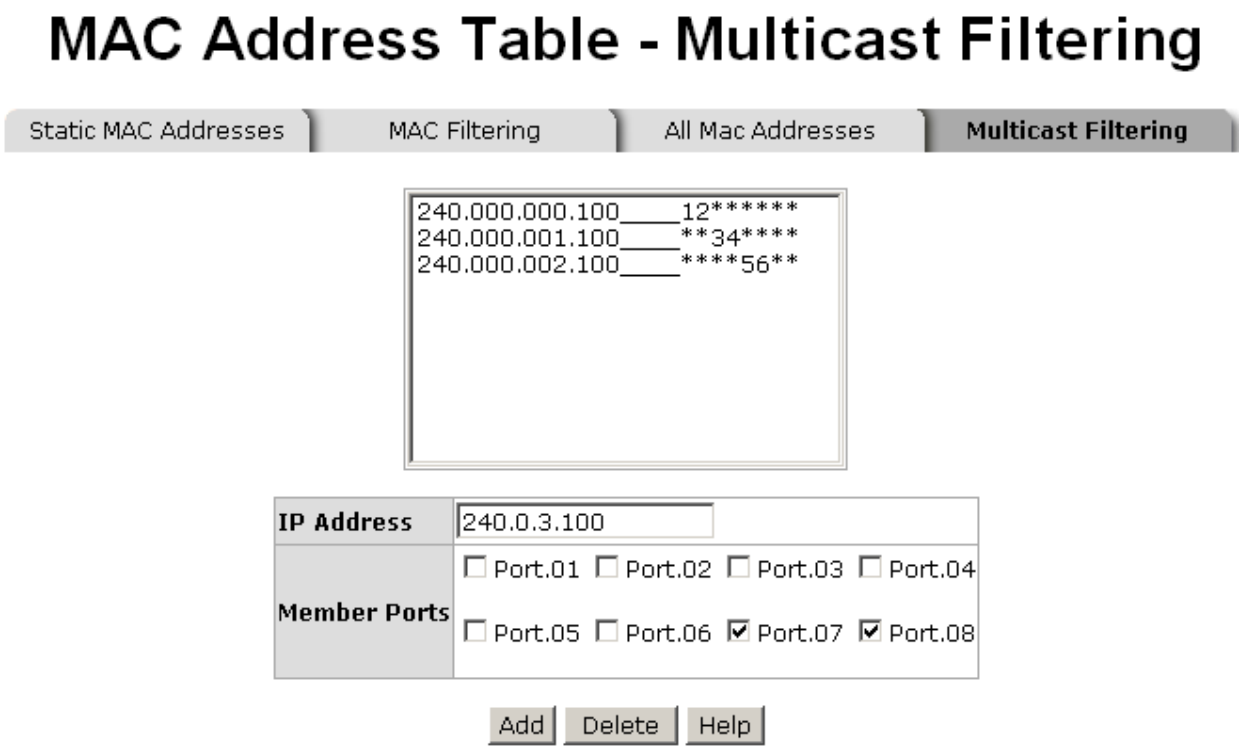


All MAC Address interface

MAC Address Table—Multicast Filtering

Multicasts are similar to broadcasts. They are sent to all end stations on a LAN or VLAN. Multicast filtering determines which end stations can receive the multicast traffic if the connected ports had been included in the specific multicast groups. With multicast filtering, network devices only forward multicast traffic to the ports that are connected to the registered end stations.

- **IP Address**: Assign a multicast group IP address in the range of 224.0.0.0 ~ 239.255.255.255.
- **Member Ports**: Tick the check box beside the port number to include them as the member ports in the specific multicast group IP address.
- Click Add to append a new filter of multicast to the field, or select the filter in the field and click Delete to remove it.



Multicast Filtering interface

Factory Default

Reset switch to default configuration. Click Reset to reset all configurations to the default value.

Factory Default interface

Save Configuration

Save all configurations that you have made in the system. Click Save to save the all configuration to the flash memory.

Save Configuration interface

System Reboot

Reboot the switch in software reset. Click Reboot to reboot the system.

System Reboot interface

Troubleshooting

- Verify the switch is using the right power cord/adapter (DC 12-48V), please don't use the power adapter with DC voltage higher than 48V, or it may damage the switch.
- Select the proper UTP cable to construct user network. Please check that is using the right cable. Use unshielded twisted-pair (UTP) or shield twisted-pair (STP) cable for RJ-45 connections: 100Ω Category 3, 4 or 5 cable for 10Mbps connections, 100 Ω Category 5 cable for 100Mbps connections, or 100Ω Category 5e/6 cable for 1000Mbps connections. Also be sure that the length of any twisted-pair connection does not exceed 100 meters (328 feet).
- **Diagnosing LED Indicators:** The Switch can be easily monitored through panel indicators, which indicate common problems. Check the switch panel LEDs to assist in identifying problems.
- If the power indicator does not light on when the power cord is plugged in, there may be a problem with the power cord. Check for loose power connections, power losses or surges at power outlet. If user still cannot resolve the problem, contact user local dealer for assistance.
- If the Industrial switch LED indicators are normal and the connected cables are correct but the packets still cannot transmit, Please check configuration or status.

Technical Specification

The 6 10/100/1000T + 2 10/100/1000T/ 100/1000 SFP Combo w/ X-Ring Managed Switch technical specification is following.

Standard	IEEE 802.3 10Base-T Ethernet IEEE 802.3u 100Base-TX IEEE802.3ab 1000Base-T IEEE802.3z Gigabit fiber IEEE802.3x Flow Control and Back Pressure IEEE802.3ad Port trunk with LACP IEEE802.1d Spanning Tree IEEE802.1w Rapid Spanning Tree IEEE802.1p Class of Service IEEE802.1Q VLAN Tag IEEE 802.1x User Authentication (Radius) IEEE802.1ab LLDP
SNMP MIB	RFC 1215 Trap, RFC 1213 MIBII, RFC 1157 SNMP MIB, RFC 1493 Bridge MIB, RFC 2674 VLAN MIB, RFC 1643, RFC 1757, RSTP MIB, Private MIB, LLDP MIB
Back-Plane (Switching Fabric)	16 Gbps
Packet throughput ability	23.8Mpps at 64bytes
Technology	Store and forward switching architecture
Transfer Rate	14,880 pps for 10Base-T Ethernet port 148,800 pps for 100Base-TX/FX Fast Ethernet port 1,488,000 pps for Gigabit Ethernet port

Packet Buffer	1Mbits
MAC address	8K MAC address table
Flash ROM	4Mbytes
DRAM	32Mbytes
Connector	10/100/1000TX: 6 ports RJ-45 with Auto MDI/MDI-X function 10/100/1000T/Mini-GBIC Combo: 2 x RJ-45 + 2 x 100/1000 SFP sockets RS-232 interface: RJ-45 type
Network Cable	10/100/1000Base-T: 2-pair UTP/STP Cat. 5e/6 cable EIA/TIA-568 100-ohm (100m) SFP (Mini-GBIC): Multi-mode: 50/125μm~62.5/125μm Single-mode: 9/125μm
Protocol	CSMA/CD
LED	**Per port:** Link/Activity (Green), Speed 1000M (Green) **SFP (Mini-GBIC):** Link/Activity (Green) **Per unit:** Power (Green), Power 1 (Green), Power 2 (Green), Fault (Red), Master (Green)
Power Supply	Input Power Isolation design for Telecom application 12 ~48 VDC Redundant power and removable terminal block
Power Consumption	18 Watts

Install	DIN rail kit for DIN-type cabinet and wall mount ear for wall mount install
Operation Temp.	-10°C to 60°C (14°F to 140°F)
Operation Humidity	5% to 95% (Non-condensing)
Storage Temperature	-40°C to 85°C
Case Dimension	IP-30, 72 mm (W) x 105 mm (D) x 152mm (H)
EMI	FCC Class A CE EN61000-4-2 (ESD) CE EN61000-4-3 (RS) CE EN61000-4-4 (EFT) CE EN61000-4-5 (Surge) CE EN61000-4-6 (CS) CE EN61000-4-8 CE EN61000-4-11 CE EN61000-4-12 CE EN61000-6-2 CE-EN61000-6-4
Safety	UL, cUL, CE/EN60950-1
Stability testing	IEC60068-2-32 (Free fall) IEC60068-2-27 (Shock) IEC60068-2-6 (Vibration)
X-Ring	Supports X-Ring, Dual Homing, and Couple Ring Provides redundant backup feature and recovery time from failure less than 300ms
VLAN	Port based VLAN IEEE802.1Q Tag VLAN (256 entries)/VLAN ID (up to 4 K, VLAN ID can be assigned from 1 to 4096)

	GVRP (256 Groups) Double Tag VLAN (Q in Q)* Private VLAN**
Port Trunk with LACP	LACP Port Trunk: 4 Trunk groups/Maximum 4 trunk members
Class of service	IEEE802.1p class of service Per port provides 4 priority queues.
Quality of service	The QoS determined by port, Port based/Tag based, IPv4/IPv6 Different Service
Spanning tree	IEEE802.1d spanning tree IEEE802.1w rapid spanning tree.
Port mirror	TX packet only, RX packet only, Both of TX and RX packet
IGMP	IGMP snooping v1, v2 Up to 256 multicast groups and IGMP query
Bandwidth control	■ Ingress packets filter and egress packet limit. ■ The egress rate control supports all of packet type and the limit rate is in the range of 100 kbps to 102400 kbps or to 256000 kbps for giga ports, and zero means no limit. ■ Ingress filter packet type combination rule for Broadcast/Multicast/Flooded Unicast packet, Broadcast/Multicast packet, Broadcast packet only and all of packet. ■ The ingress packet filter rate range is from 100 kbps to 102400 kbps or to 256000 kbps for giga ports, and zero means no limit.
IP security	Supports 10 IP addresses that have permission to access the switch management and to prevent unauthorized intruder
Login Security	Supports IEEE802.1X Authentication/RADIUS

SNTP	Supports Simple Network Time Protocol to synchronize system clock in Internet.
SNMP Trap	Up to 3 Trap stations Cold start Port link Up Port link down Authentication Failure Private Trap for power status Port Alarm configuration Fault alarm X-Ring topology change
Relay Alarm	One relay output for port breakdown and power fail Alarm Relay current carry ability: 1A @ DC24V
DHCP client	Provide DHCP Client/ DHCP Server/IP Relay functions
Firmware update	TFTP firmware update
Configuration upload/download	Supports binary configuration file for system quick installation

* Future release

** Optional

Appendix

10 /100BASE-TX Pin outs

With10/100BASE-TX cable, pins 1 and 2 are used for transmitting data, and pins 3 and 6 for receiving data.

- **RJ-45 Pin Assignments**

Pin Number	Assignment
1	Tx+
2	Tx-
3	Rx+
6	Rx-

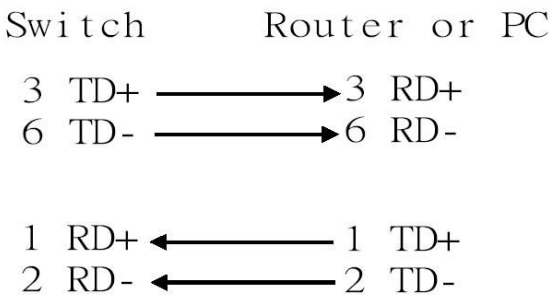
[NOTE] "+" and "-" signs represent the polarity of the wires that make up each wire pair.

The table below shows the 10 / 100BASE-TX MDI and MDI-X port pin outs.

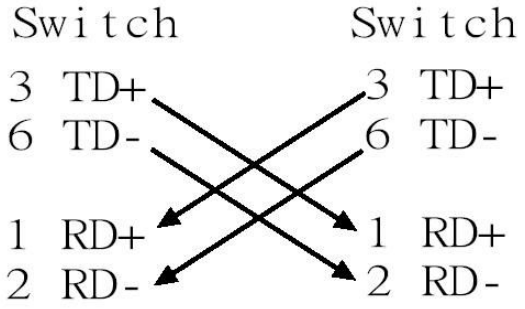
Pin MDI-X	Signal Name	MDI Signal Name
1	Receive Data plus (RD+)	Transmit Data plus (TD+)
2	Receive Data minus (RD-)	Transmit Data minus (TD-)
3	Transmit Data plus (TD+)	Receive Data plus (RD+)
6	Transmit Data minus (TD-)	Receive Data minus (RD-)

10/100Base-TX Cable Schematic

The following two figures show the 10/100Base-TX cable schematic.



Straight-through cable schematic

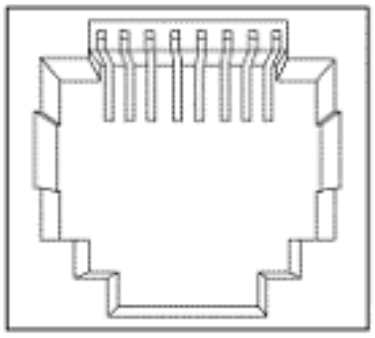


Cross over cable schematic

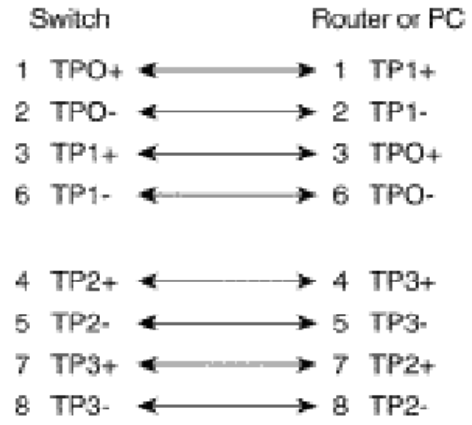
10/100/1000Base-TX Pin outs

The following figure shows the 10/100/1000 Ethernet RJ-45 pin outs.

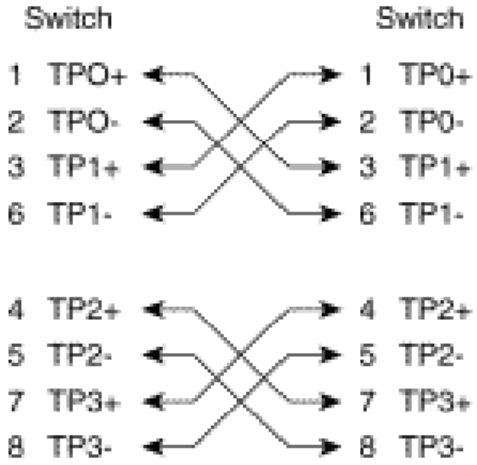
Pin	Label
1	TP0+
2	TP0-
3	TP1+
4	TP2+
5	TP2-
6	TP1-
7	TP3+
8	TP3-



10/100/1000Base-TX Cable Schematic



Straight through cables schematic



Cross over cables schematic

Gigabit Copper/SFP (mini-GBIC) combo port

The Industrial switch has two auto-detect Giga port—UTP/Fiber combo ports. The Gigabit Copper (10/100/1000T) ports should use Category 5e or above UTP/STP cable for connection. The SFP slots are for connecting to the network segment with single or multi-mode fiber. You can choose an appropriate mini-GBIC module to plug into the slots.

Make sure the module is aligned correctly and then slide the module into the SFP slot until a click is heard. You should use proper multi-mode or single-mode fiber according to the used SFP module. Fiber optic connections enable transmit speeds up to 1000 Mbps, while preventing electrical noise interference and permitting transmission distance up to 110 km, depending on the mini-GBIC module.

The small form-factor pluggable (SFP) is a compact optical transceiver used in optical communications for both telecommunication and data communications applications.
To connect the transceiver and LC cable, please follow the steps shown below:

First, insert the transceiver into the SFP slot. Notice that the triangle mark is the bottom of the slot.

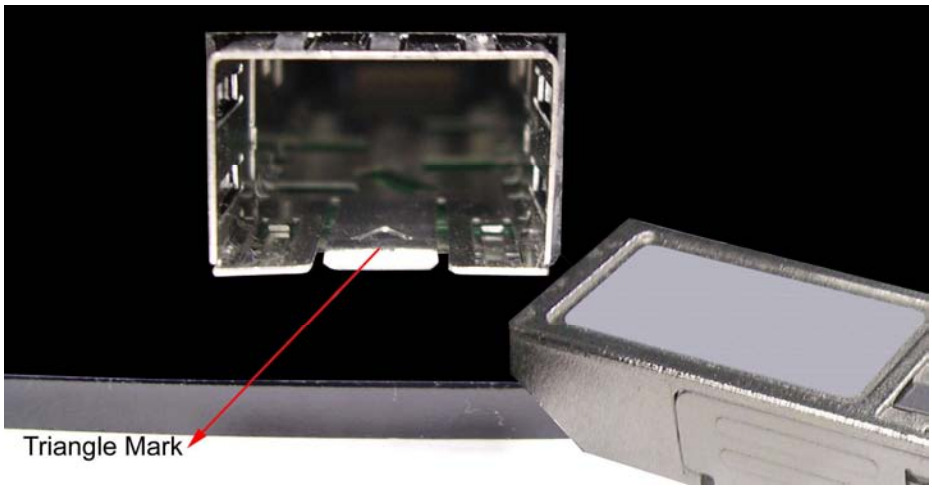


Figure 2.8: Transceiver to the SFP slot

Figure 2.9: Transceiver Inserted

Second, insert the fiber cable of LC connector into the transceiver.

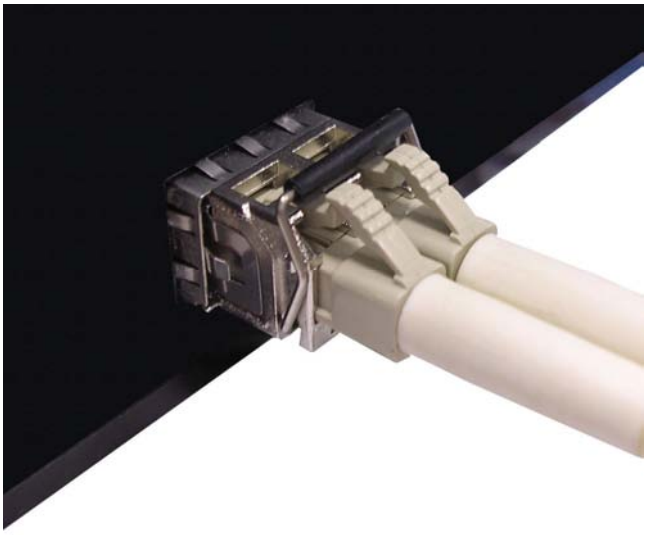


Figure 2.10: LC connector to the transceiver

To remove the LC connector from the transceiver, please follow the steps shown below:

First, press the upper side of the LC connector to release from the transceiver and pull it out.

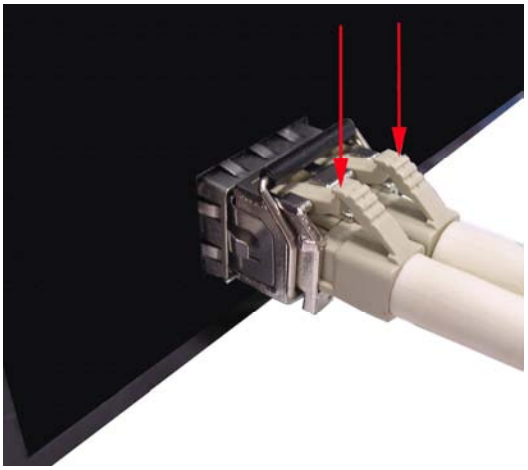


Figure 2.11: Remove LC connector

Second, push down the metal loop and pull the transceiver out by the plastic handle.

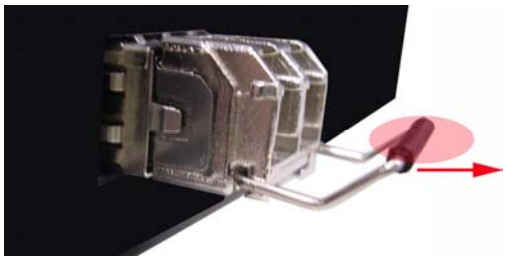


Figure 2.12: Pull out from the transceiver

Cabling

- Use four twisted-pair, Category 5e/above cabling for RJ-45 port connection. The cable between the switch and the link partner (switch, hub, workstation, etc.) must be less than 100 meters (328 ft.) long.
- Fiber segment using **single-mode** connector type must use 9/125 µm single-mode fiber cable.
- Fiber segment using **multi-mode** connector type must use 50 or 62.5/125 µm multi-mode fiber cable.